GONÇALO NUNO CORREIA ZAMBUJO SERRÃO

CYBERBULLYING: A PRIMEIRA RESPOSTA ÀS VÍTIMAS

Dissertação com vista à obtenção do grau de
Mestre em Direito e Segurança

Orientador:
Doutor Ricardo Teresa Ribeiro, Professor da Escola Superior de Tecnologia da Saúde de Lisboa

Julho, 2019

Declaração Anti Plágio

Eu, Gonçalo Nuno Correia Zambujo Serrão, declaro por minha honra que o documento intitulado "*CYBERBULLYING*: A PRIMEIRA RESPOSTA ÀS VÍTIMAS" corresponde ao resultado da investigação por mim desenvolvida no âmbito do Curso de Mestrado em Direito e Segurança e que é um trabalho original, em que todos os contributos estão corretamente identificados em citações e nas respetivas referências bibliográficas.

Tenho consciência que a utilização de elementos alheios não identificados constitui grave falta ética, moral, legal e disciplinar.

Julho de 2019

Gonçalo Nuno Correia Zambujo Serrão

Epígrafe

"Espero que estejam preparados, porque estou prestes a contar-vos a história da minha vida. Mais concretamente, os motivos que conduziram ao fim da minha vida. E se estiverem a ouvir estas cassetes, vocês são um desses motivos"

(Asher, 2017, p. 15)

Dedicatória

Às Anas, mulher e filha, que permitiram a realização deste trabalho.

A todas as vítimas de *cyberbullying* que necessitam de uma resposta.

Agradecimentos

Encontro-me perante o culminar de um ciclo que se revelou bastante interessante realizar, mas que não teria sido possível sem o apoio e acompanhamento dos diferentes intervenientes, daí que gostaria de deixar os meus agradecimentos a todos que, de forma direta e indireta, contribuíram para a sua realização.

Desta forma, começaria por agradecer a maneira profissional e profícua de todos os professores que ministraram a componente letiva do curso em apreço, em particular do Professor Lino Santos, que através Unidade Curricular de Cibersegurança, partilhou conhecimento que serviu de base à presente investigação.

Ao Professor Doutor Ricardo Ribeiro, pela permanente disponibilidade, orientação no trabalho e saber transmitido, fundamentais na realização desta dissertação.

Igualmente ao Sr. Tenente-Coronel Gonçalo Carvalho, pelo inexcedível apoio, contributo e partilha de conhecimento, essenciais para a persecução dos objetivos definidos.

A todos os entrevistados, pela disponibilidade, experiência e conhecimento partilhado, em especial ao Sr. Inspetor Baltazar Rodrigues, do qual devo realçar o imprescindível e valioso contributo nas abordagens sobre a problemática em causa.

Por fim, à minha família, pelo apoio e incentivo, essencialmente pela compreensão da ausência.

Resumo

O *cyberbullying é* um fenómeno atual que afeta crianças e jovens, levando à sua destruição emocional, social e física.

O crescimento das novas tecnologias, associadas à conectividade digital e partilha de informação, permitiram o desenvolvimento de um novo espaço de interação e socialização, o ciberespaço, que transpõe a vida real para um mundo virtual.

O aumento das práticas sociais no ciberespaço levou também ao aumento de fenómenos como o *cyberbullying*. Dadas as características do ciberespaço, as agressões virtuais inerentes ao *cyberbullying,* tornam-se difíceis de combater e as suas consequências tendem a ser devastadoras para as vítimas, maiores consoante o período que se mantenham *online*.

Neste contexto, surge o objetivo geral da presente investigação: identificar e caracterizar a primeira resposta às vítimas de *cyberbullying,* procurando como intervir de imediato nestes casos, e assim garantir uma maior proteção da vítima e minimizar os efeitos da agressão.

Como metodologia, partiu-se de um raciocínio dedutivo, que permitiu, através de investigações, abordagens teóricas e reflexões sobre o problema, encontrar uma verdade. Por conseguinte, mediante uma análise de conteúdo através da observação qualitativa dos dados reunidos, foi possível o desenvolvimento das conclusões.

Desta forma, constatou-se a importância de existir um maior controlo do ciberespaço por parte dos seus intervenientes e a necessidade de uma intervenção imediata para garantir a proteção e apoio das vítimas, partindo essencialmente do empenhamento e cooperação entre os responsáveis e o desenvolvimento de uma capacidade ciberpolicial.

Palavras chave:

Ciberespaço, Agressões Virtuais, *Cyberbullying*, Primeira Resposta.

Abstract

Cyberbullying is a current phenomenon that is affecting children and young people, leading to their emotional, social and physical destruction.

The growth of new technologies, combined with digital connectivity and information sharing, has developed a new space for interaction and socialization, the cyberspace, which transposes real life into a virtual world.

The rise of social practices in cyberspace has also led to the rise of phenomenons such as cyberbullying. The features of cyberspace turns the virtual aggressions of cyberbullying difficult to face and their consequences should be devastating to the victims, longer the period they keep online.

In this context comes the objective of this investigation: identify and characterize the first response to the cyberbullying victims, seeking how to face it immediately in this cases, and keep the greatest protection to the victim and minimize the aggression effects.

The methodology started by a deductive reasoning, which allowed, through investigations, theoretical approaches and reflections on the problem, to find a truth. For one, through a data analysis by qualitative observation of the obtained information, it was possible to develop the conclusions.

Thus, it was verified that is importance a bigger control of the cyberspace by the stakeholders and a immediate intervention to provide protection and support to victims, essentially based on the commitment and cooperation between those who are responsible and the development of a cyberpolice capability.

Keywords:

Cyberspace, Virtual Aggressions, Cyberbullying, First Response.

Índice Geral

Índice de Quadros

Lista de Apêndices

Lista de abreviaturas, siglas e acrónimos

Art.º - Artigo

ANACOM - Autoridade Nacional de Comunicações

Cap. - Capítulo

CERT - *Computer Emergency Response Team*

cit. - Citado

CM/Rec - Recomendação do Comité de Ministros

CNCS - Centro Nacional de Cibersegurança

CPP - Código de Processo Penal

CRP - Constituição da República Portuguesa

Dec. - Decreto

E - Entrevistado/a

et al. - e outros

EU - União Europeia

EUA - Estados Unidos da América

FCCU - *Federal Computer Crime Unit*

FCT - Fundação para a Ciência e a Tecnologia

FDUNL - Faculdade de Direito da Universidade Nova de Lisboa

FS - Forças de Segurança

GNR - Guarda Nacional Republicana

IP - Protocolo da Internet

IPDJ - Instituto Português do Desporto e Juventude.

ISP - *Internet Service Providers*

LOIC - Lei de Organização da Investigação Criminal

LPC - Lei de Política Criminal

OE - Objetivos Específicos

OG - Objetivo Geral

OPC - Órgãos de Polícia Criminal

p. - Página

pp. - Páginas

PD - Pergunta Derivada

PJ - Polícia Judiciária

PP - Pergunta de Partida

RCCU - *Regional Computer Crime Units*

TIC - Tecnologias de Informação e Comunicação.

UGC - *User Generated Content*

UNC3T - Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica

INTRODUÇÃO

A evolução das Tecnologias de Informação e Comunicação (TIC) e a conectividade permitida pela internet, levaram a que o ser humano também passasse a desenvolver as suas atividades socias no ciberespaço. Esta nova dimensão, para além de criar um novo espaço de vivência social, apresenta características muito próprias. Foram assim criadas novas formas de comunicação e interação entre as pessoas, e, no caso em particular, entre as crianças e jovens que têm acesso às TIC.

O *bullying* tem sido um fenómeno global que tem preocupado autoridades, diferentes entidades que lidam com crianças e jovens, e em especial famílias devastadas pelos seus efeitos. Trata-se de um problema que tem provocado graves danos nas vítimas, tanto a nível social e emocional como físico, levando por vezes a depressões profundas que poderão levar à ocorrência de suicídios.

Face ao desenvolvimento das TIC, também o *bullying*, à semelhança de outras práticas socias e criminais, migrou para o ciberespaço, personificando agora as suas agressões de forma virtual, denominando-se por *cyberbullying*. Por sua vez, o contexto digital em que as agressões agora ocorrem, vem facilitar o comportamento do agressor, como pode aumentar a incidência das agressões e as suas consequências.

A potencialidade de uma agressão em contexto digital pode ser devastadora para a vítima, o que impõe uma abordagem a este fenómeno e se perceba a necessidade de intervenção imediata aquando de uma ocorrência.

O presente estudo propõe-se a investigar o "vazio" existente no combate ao *cyberbullying* e procurar de que forma poderá ser mitigado o contexto potenciador das agressões virtuais e dos seus efeitos.

A maioria dos estudos e trabalhos identificados, descritos em maior detalhe no capítulo 1., direciona-se para a caracterização do fenómeno e para a sua prevenção, o que não é suficiente, dado que em caso de ocorrência, a escalabilidade da agressão poderá não ter fim, levando a questionar qual a resposta necessária para este tipo de ocorrência.

Desta forma, sendo este fenómeno conjuntural e uma preocupação crescente face à necessidade de resposta, define-se como Objetivo Geral (OG) para a presente

investigação, identificar e caracterizar a primeira resposta às vítimas de *cyberbullying*, procurando-se aumentar o corpo de conhecimento sobre esta temática com a finalidade de garantir uma maior proteção da vítima e minimizar os efeitos da agressão.

De forma a contribuir para atingir este objetivo, foram definidos os seguintes Objetivos Específicos (OE):

OE1: Descrever como se poderão cessar as agressões virtuais de *cyberbullying;*

OE2: Descrever como se poderão identificar os autores de agressões virtuais de *cyberbullying;*

OE3: Identificar os mecanismos para recolher e preservar a prova digital de agressões virtuais de *cyberbullying;*

OE4: Identificar as ações que poderão ser tomadas para apoiar as vítimas de agressões virtuais de *cyberbullying*.

Para o desenvolvimento deste trabalho, utilizou-se um modelo de análise que se baseou em perguntas de investigação. Considerando o enquadramento até então, levantou-se a seguinte Pergunta de Partida (PP) - Qual a resposta imediata que as vítimas de *cyberbullying* necessitam?

Derivadas da PP e no sentido de melhor contribuir para a sua resposta, formularam-se as seguintes Perguntas Derivadas (PD):

PD 1 - De que forma poderão ser cessadas as agressões virtuais de *cyberbullying*?

PD 2 - De que forma poderão ser identificados os autores de agressões virtuais de *cyberbullying*?

PD 3 - Quais os mecanismos para obter prova das agressões virtuais de *cyberbullying*?

PD 4 - Quais as ações a serem tomadas para apoiar as vítimas de agressões virtuais de *cyberbullying*?

A fim de contribuir para os objetivos propostos, partiu-se de um raciocínio dedutivo, onde as teorias deram lugar a uma realidade particular, ou seja, a partir de investigações, abordagens teóricas e reflexões sobre o problema, procurou-se uma verdade. O processo de investigação em si assenta numa estratégia qualitativa para

obter a informação necessária, recorrendo a estudos, reflexões e conhecimentos de especialistas na matéria.

Iniciou-se este processo de investigação com uma fase exploratória, analisando a conjuntura atual através de publicações sobre o tema, que permitiram a identificação do problema a investigar, seguindo-se então uma revisão da literatura existente. Para obter mais informação, procedeu-se à fase analítica, partindo da recolha, registo e tratamento de dados provenientes de um inquérito por entrevista semiestruturada ou semidiretiva, aplicado a um conjunto de especialistas. As respostas à entrevista foram objeto de uma análise de conteúdo e confrontadas com o enquadramento teórico do trabalho, possibilitando assim a resposta às PD e PP, e as consequentes conclusões.

Nesse sentido, organizou-se o presente trabalho em quatro capítulos. No primeiro capítulo é efetuado um enquadramento teórico com uma revisão de literatura sobre o tema em investigação. Essencialmente sobre os principais conceitos, perspetivas teóricas e pesquisas relevantes para o objeto de estudo. Segue-se o segundo capítulo com a demonstração da metodologia utilizada, desde o raciocínio ao tipo de abordagem, ao modelo de análise e aos métodos de recolha e análise de dados.

O terceiro capítulo faz a apresentação e análise dos resultados, comparando com os estudos abordados no enquadramento teórico, que acabam por realçar os aspetos relevantes desses resultados.

Dos comentários permitidos pelos resultados da investigação, o presente trabalho termina com as conclusões e reflexões, constituindo-se como a súmula aos principais tópicos abordados e que respondem a achados que garantem maior proteção das vítimas de *cyberbullying* e a forma de minimizar os efeitos das agressões virtuais. Por fim, encerra-se com as reflexões que permitem apontar caminhos de como será possível operacionalizar a resposta imediata para o problema.

1. ENQUADRAMENTO TEÓRICO

1.1. O Ciberespaço

1.1.1. Enquadramento

"*O ciberespaço é o campo de batalha do futuro"*, Leon Panetta, Secretário da Defesa dos EUA (2014)[1]

O desenvolvimento da internet e o facto da mesma se encontrar em todas as atividades da sociedade atual, levou à criação de uma sociedade em rede, permitindo a conetividade entre o mundo físico e o virtual. A sua evolução permitiu uma conectividade global de informação, que hoje traduz uma representação do mundo real e a constituição do denominado ciberespaço.

Em termos genéricos, Santos (2017)[2] considera que o ciberespaço se traduz num mundo virtual, numa rede informática de dados, num media, numa rede social, numa sociedade de informação ou uma biblioteca global.

O Prefixo "*Ciber*" teve origem em 1948, por Norbert Wiener, no livro *Cybernetics*, definindo como a interface ou interação entre o Homem e a máquina, que produz um novo ambiente ou um ambiente alternativo. Pode alargar-se o conceito e falar-se no ambiente que resulta da interação entre o homem e a tecnologia. Já o termo "Ciberespaço" foi utilizado pela primeira vez por Gibson em 1984, referindo-se ao ciberespaço como uma alucinação consensual experimentada por biliões de operadores, uma representação gráfica de dados extraídos de bancos de cada computador do sistema humano. Em suma, uma alucinação coletiva sobre um ambiente de comunicação de dados abstratos (Santos, 2017).

O conceito de Ciberespaço iniciou-se com o computador pessoal, seguindo-se o desenvolvimento da Internet e posteriormente o desenvolvimento de aplicações, com destaque para a Web 2.0 e as redes sociais. Em determinado momento, os

[1] *In* Strategia. *Revista da Armada*, abril, 2016, p. 4.
[2] Cibersegurança. Aula 1 da Unidade Curricular – Cibersegurança, no âmbito do Mestrado em Direito e Segurança, 2016/2017, da FDUNL.

Estados[3] começaram a perceber que a internet era uma forma de melhor prestar os seus serviços, surgindo a possibilidade da criação do governo eletrónico. Neste sentido, a sociedade evoluiu muito ao nível da disponibilização de informação na internet. Contudo, devido há falta de literacia digital, em particular na faixa etária superior aos 65 anos, ainda não foi possível retirar o melhor proveito deste desenvolvimento (Santos, 2017).

Ao nível do controlo, o ciberespaço caracteriza-se por ser um espaço altamente permeável, uma tentação para os Estados e uma realidade para as grandes empresas. Neste momento estamos perante um negócio rentável com a venda de dados e os *likes* pessoais dos utilizadores a outras empresas. Se os dados são divulgados e acumulados algures no ciberespaço, certamente vão ser usados (Santos, 2017).

Pode enquadrar-se o ciberespaço em três estruturas: o ciberespaço físico, que se refere à matéria da qual são feitos os computadores, periféricos associados e os seus utilizadores (Gozzi, 1994 cit. por Santos, 2017); o ciberespaço conceptual, que se traduz na noção de espaço criado na mente, resultante da interação com os computadores e as tecnologias da informação (Bolter e Gibson, 1984, cit. por Santos, 217); e ainda o ciberespaço percetual, que é "o sentimento de espaço captado pelos nossos sentidos, criado pelo interface homem – máquina" (Barnes, 1995 cit. por Santos, 2017).

O ciberespaço apresenta algumas características distintivas. O termo apela ao imaginário, dado que transporta o recetor para a relação com as tecnologias, é aterritorial, visto que não respeita fronteiras, levantando imensos problemas de delimitação de conceitos como jurisdição ou propriedade. Outra característica é o facto de ser orgânico, fruto de estar em constante mutação, na medida em que tem uma estrutura governada por uma rede de atores que não são só Estados. Sempre que há um novo media, pensa-se que a relação entre os Estados e os cidadãos será nivelada, o que se revela uma utopia libertária. Como última característica deste espaço virtual está a possibilidade de realização de ações de forma praticamente

[3] Entidade responsável pela estrutura e pela organização política e administrativa de um território e sua população, ou conjunto de populações, garantindo a existência de um país soberano, reconhecido internacionalmente pelos seus pares. *In* https://www.infopedia.pt/dicionarios/lingua-portuguesa/estado.

anónima, levantando dificuldades na atribuição dos atos praticados ou à identificação dos seus autores (Santos, 2017).

No entanto, o termo ciberespaço tem-se definido de uma forma muito vaga. Assim, o mesmo é usado por grupos ou comunidades para se referirem a uma rede planetária de computadores, a possibilidade de realizar atividades pela internet, o ambiente virtual imersivo de lazer e cultura, o produto das interações sociais mediadas pelas tecnologias da informação, ou o local onde é armazenada e processada a informação (Guedes e Santos, 2015).

Já Antunes e Rodrigues (2018, p. 102), consideram o ciberespaço como "o espaço virtual que é criado através das comunicações e dos meios tecnológicos disponíveis, sem intervenção humana."

Segundo Nunes (2014), o ciberespaço tornou-se um verdadeiro mediador das relações sociais e um motor do desenvolvimento económico dos países mais desenvolvidos. O ciberespaço não tem fronteiras definidas e utiliza como porta de acesso a internet. O espaço físico perde significado e a comunicação entre os homens passa a ser dirigida pelo tempo de interação, num espaço virtual onde a informação está disponível online, independentemente do local e da hora do dia.

Pode considerar-se o ciberespaço como um domínio virtual, concebido pelo ser humano, mas que depende de um suporte físico, como por exemplo, sistemas de comunicação, sistemas de informação e outros sistemas eletrónicos (Monteiro, 2016).

A importância do ciberespaço tem vindo a aumentar gradualmente, fazendo parte do quotidiano da maioria da população mundial, nas diferentes dimensões da sociedade.

Segundo Monteiro (2016), no final de 2015, os utilizadores da internet já constituíam quase metade da população mundial, em que para muitas pessoas e organizações, a conectividade ao ciberespaço já se tornara uma necessidade básica. Daí que seja possível verificar uma mudança do mundo real para o mundo virtual, potenciando, inevitavelmente, o bem estar económico e social da população, mas também a transição e adaptação dos problemas da sociedade para este mundo virtual globalizado, como o cibercrime ou mesmo a ciberguerra.

1.1.2. Ameaças no Ciberespaço

O surgimento das Tecnologias de Informação e Comunicação (TIC) trouxeram inegáveis consequências positivas para a sociedade. No entanto, a utilização destas ferramentas e a aproximação que as mesmas trouxeram entre pessoas e Estados, quebrando barreiras e fronteiras, leva a que se explorem vulnerabilidades, criando riscos sociais e materiais a fim de se obterem vantagens sobre terceiros.

O ciberespaço transpõe a vida real para um mundo virtual, com novas formas de interação, projetando um mundo em rede e com um conjunto de novas ameaças. Fruto do seu carácter, este mundo levou assim ao desenvolvimento de novos modos de atuação e ao desenvolvimento de um novo espectro de ameaças.

De acordo com Santos (2011), essas atividades podem ser divididas em diferentes categorias, de acordo com a motivação e o perfil dos seus autores, nomeadamente:

- o cibercrime, em que o computador, a forma digital e os sistemas informáticos estão na base do comportamento criminoso;
- a desobediência civil eletrónica e *hacktivismo*, em que indivíduos politicamente motivados usam a internet como meio para promover e catalisar as suas causas e disseminar a sua mensagem;
- o ciberterrorismo, na medida que um ciberatentado pode interromper infraestruturas críticas e sistemas essenciais a uma sociedade;
- a ciberguerra, a fim de garantir o uso da violência entre grupos organizados politicamente, fazendo uso de todos os instrumentos disponíveis para atingir os objetivos políticos, em particular para garantir superioridade de informação e afetando os sistemas de informação e infraestruturas críticas do adversário.

1.2. O Cibercrime

A evolução tecnológica e a internet permitiram grande desenvolvimento na comunicação e propaganda ideologista, sejam discursos sociais, culturais, religiosos ou mesmo de ódio.

Destacando Schmidt e Cohen (2013), deve estar-se atento aos impactos da cibercriminalidade e mesmo a questões mais complexas como o terrorismo. Poder-se-á ver num futuro próximo os utilizadores do ciberespaço a abdicar voluntariamente de direitos no mundo fisico, como privaciadade, segurança, dados pessoais, com a finalidade de beneficiarem de uma conexaão ao mundo virtual. Contudo, o otimismo apenas crescerá a partir do travão que tecnologia e conectividade podem constituir contra os abusos, o sofrimento e a destruição do nosso mundo.

A cibercriminalidade ganha assim relevo, fruto da expansão dos meios tecnológicos e da internet, reunindo toda a criminalidade que possa ser efetuada por meios informáticos. Não obstante, a prática deste fenómeno atinge várias dimensões e caracteriza-se por ser de difícil deteção fruto das suas caracteristicas.

Segundo Natário (2013), pode identificar-se um conjunto de características inerentes ao cibercrime, nomeadamente: a sua transnacionalidade, na medida em que não existe necessidade de proximidade física entre vítimas e atacantes, apenas existe necessidade de um computador ligado à internet; o anonimato, fruto da dificuldade em identificar os cibercriminosos, e mesmo que sejam, a recolha de provas e a detenção dos suspeitos estão condicionadas à vontade de colaboração dos países a partir dos quais o crime foi cometido; a tecnologia, devido ao facto deste tipo de crime poder ser automatizado, porque através de uma ação podem ser cometidos milhares de crimes de forma expedita e sem esforço; a organização, que cresce entre cibercriminosos, permitindo alianças e recrutamentos; e o impacto, que pode ser criado com os incidentes, e que possivelmente ainda não existe capacidade de avaliar com rigor a verdadeira dimensão dessa ameaça.

Para Santos (2011), as TIC têm facilitado, fruto das suas carcaterísticas, explorar as vulnerabilidades inerentes à utilização do ciberespaço e dos sitemas informáticos. Não obstante, também as características intrínsecas do ciberespaço colocam grandes desafios ao combate ao cibercrime, nomeadamente a velocidade ou

instantaneidade de execução deste tipo de crimes, o carácter praticamente anónimo das transações, o perfil não determinístico do percurso das comunicações na internet e a volatilidade, cifra e dispersão nos registos que podem vir a ser úteis numa investigação criminal.

1.2.1. Conceito

"*É assim a Internet: o maior espaço sem lei do mundo*" (Schmidt e Cohen, 2013, p.14).

O número de acessos à internet aumenta diariamente, um dia toda a população estará *online* e a navegar no ciberespaço (Schmidt e Cohen, 2013).

As TIC têm vindo a permitir uma evolução desmedida nas populações, empresas e Estados, levando a um descontrolo no acesso e divulgação de informação.

Os Direitos, Liberdades e Garantias de uma sociedade cibernética, acabarão por ser balanceados com estratégias securitárias, a fim de reprimir atos ilicitos. Da mesma forma que um criminoso atua sem cumprir limitações legais, também as forças securitárias estatais que têm por missão garantir a segurança no ciberespaço, deverão atuar regulamentadas por uma componente legal adequada, permitindo que estejam altamente especializadas e capazes de explorar as potencialidades dos sistemas informáticos.

Todo o desenvolvimento tecnológico e consequente rede massiva de conexões levará a um aumento significativo e descontrolado de informação no ciberespaço, levando a que os cidadãos não consigam garantir o controlo da sua informação. Desta forma, enfrenta-se o desafio de compreender o que estamos dispostos a fazer para garantir o controlo, segurança e privacidade sobre toda essa informação, bem como a integridade dos sistemas que garantem a conectividade e a globalização cibernética.

Fruto da expansão dos meios tecnológicos e em particular da internet, encontra-se também uma crescente dimensão do cibercrime. Pode considerar-se que a passagem da vivência real das populações para um mundo virtual também levou a uma migração da criminalidade, que em determinados aspetos conseguem a sua

associação, dado que os seus autores podem praticar os crimes tradicionais, ou mesmo novos crimes, proporcionados pelas novas tecnologias (Venâncio, 2011).

No entanto, o cibercrime levanta diferentes questões relativamente ao seu conceito, mas no fundo são aproximados os pontos de vista deste fenómeno.

Segundo Martins, Brenner e Schwerha cit. por Santos (2011), o cibercrime é "todo o acto em que o computador serve de meio para atingir um objectivo criminoso ou em que o computador é o alvo desse acto". Neste caso, o cibercrime reúne toda a criminalidade que pode ser perpetrada por meios informáticos.

A prática de crimes na internet assume várias denominações, entre elas, crime digital, crime informático, crime informático-digital, *high technology crimes*, *computer related crime*. Não existe consenso quanto à expressão, quanto à definição, nem mesmo quanto à tipologia e classificação destes crimes. Contudo, atendendo aos diversos instrumentos legislativos, estes podem ser enquadrados na denominação de cibercrime (Simas, 2014).

Para Peter Garbosky cit. por Santos (2011), estes crimes podem ser divididos em três grupos: crimes convencionais realizados com recurso a computador; crimes convencionais em que o computador não é o instrumento principal da atividade, mas onde o meio de realização de prova assume a forma digital; e crimes em que o alvo são os sistemas informáticos. Daí que Venâncio (2011, p. 17) destaca que se pode distinguir este fenómeno criminal em crimes "que a infomática é apenas um meio para a prática do crime, outros em que a informática aparece como um elemento do tipo legal criminalmente punido." Desta forma, pode afirmar-se que a dimensão holística que a criminalidade informática pode reunir é demasiado grande, na medida em que consegue congregar todo o tipo de criminalidade que possa ser desenvolvida por meios informáticos.

Por sua vez, Antunes e Rodrigues (2018, p. 102), definem o "cibercrime como qualquer crime que aconteça no ciberespaço. No leque de crimes em causa incluem-se as ações ilícitas praticadas com recurso às redes digitais, nomeadamente a internet. Estes crimes incluem, ainda, os crimes informáticos, que são os praticados contra os sistemas informáticos, os dados e informações alojadas nos sistemas de informação".

O desenvolvimento tecnológico, aliado às potencialidades da internet, tem permitido assistir a um crescente progresso de novos instrumentos e formas para a

persecução de crimes, "não só na transferência de comportamentos ilícitos para o ambiente digital, como na tipificação de novos crimes com elementos caracterizadores de natureza digital (…) as práticas e capacidades da informática, e em particular da internet, potenciam exponencialmente a internacionalização da criminalidade" Venâncio (2011, p. 15).

O facto dos crimes informáticos terem um carácter universal fruto da conectividade global, leva a que as relações possam ser dissimuladas ou mesmo anónimas, camufladas cada vez mais por evoluções digitais dos seus agentes. Daí que, face à crescente deslocalização da vida real para o mundo virtual, em particular das relações sociais, atividades económicas e estatais, assiste-se também, como já referido, à deslocação das atividades criminosas para este espaço virtual. Por sua vez, "dia para dia, apuram-se novas técnicas de dissimulação ou ocultação que dificultam a identificação do agente das atividades criminosas por parte das autoridades" Venâncio (2011, p. 16).

1.2.2. Enquadramento legal

A integração deste fenómeno criminal no ordenamento jurídico nacional não se esgota num diploma legal. Pode verificar-se primeiramente que o Código Penal[4] prevê ilícitos criminais nesta matéria, nomeadamente, "Devassa por meio informático", "Violação de correspondência e telecomunicações" e "Burla informática e nas comunicações".

Por sua vez, a referência é a Lei n.º 109/2009 (Lei do Cibercrime)[5], de 15 de setembro, que no seu no Cap. II, Disposições Penais Materiais, criminaliza de forma mais abrangente um conjunto de práticas, nomeadamente, a "Falsidade informática", o "Dano relativo a programas ou outros dados informáticos", a "Sabotagem informática", o "Acesso ilegítimo", a "Interceção ilegítima" e a "Reprodução ilegítima de programa protegido".

[4] Dec. Lei n.º 48/95, de 15 de março, respetivamente os art.º 193.º, 194.º e 221.º.

[5] Lei n.º 109/2009, de 15 de setembro. Aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

Face à diversidade criminal praticada no ciberespaço, surge a necessidade de legislação e orientações mais adequadas e que acompanhem a evolução social e tecnológica, no sentido de se compreender, atualizar, prevenir e reprimir este fenómeno. Nesse sentido, a através da Nota Prática n.º 11/2017 de 2 de novembro, do Gabinete Cibercrime da Procuradoria-Geral da República pode efetuar-se um enquadramento mais orientado. A presente Nota aborda jurisprudência sobre o cibercrime, pretendendo atualizar as referências jurisprudenciais sobre crimes informáticos e crimes cometidos por via de sistemas informáticos. Para o efeito, foram identificados crimes como: Acesso Ilegítimo; Falsidade Informática; Burla Informática; Burla Informática – Cartões Multibanco; Reprodução Ilegítima de Programa Protegido; Usurpação; *Phishing*; Pornografia de Menores; Não Cumprimento de Obrigações Relativas a Proteção de Dados; Ilícitos em Redes Sociais; Fotografias Ilícitas; e Jogo *Online*. Nesta abordagem importa destacar que os mais relevantes para a matéria objeto de estudo são os ilícitos em redes sociais ou mesmo as fotografias ilícitas.

De acordo com a Nota Prática n.º 11/2017, de 2 de novembro, do Gabinete Cibercrime (p. 13) "a generalização da utilização da Internet e das redes sociais e, por outro lado, o aumento da capacidade e da conectividade dos equipamentos de computação e comunicação, potenciaram a divulgação, na Internet, de conteúdos suscetíveis de violarem a honra de outrem, ou a privacidade, ou o direito à imagem de terceiros."

Estas condutas têm aumentado os processos judiciais e as consequentes decisões dos tribunais. A título de exemplo, tendo em conta a referida Nota Prática n.º 11/2017, de 2 de novembro, do Gabinete Cibercrime (p. 14), O Acórdão da Relação de Guimarães de 18 de março de 2013, proferiu que "a criação, numa rede social, de um perfil em nome de outra pessoa, com inclusão de características de utilizador ofensivas da honra e consideração do "titular" do perfil, constituem crime de difamação." Da mesma forma, o Acórdão da Relação de Évora de 14 de fevereiro de 2012, decidiu que, "estando em causa a prática de crimes contra a honra por meio de comentários publicados num *blog*, o domínio do facto assiste a duas pessoas, cuja intervenção é imprescindível ao cometimento do crime: aquela que inscreve o comentário e aquela que disponibiliza o blog para o efeito e consente na respetiva

publicação. O administrador do blog gere e seleciona os comentários feitos no mesmo, pelo que tem o pleno domínio do facto. O importante não é quem causa o facto, mas quem domina a execução deste." E o Acórdão da Relação do Porto de 12 de julho de 2017, refere que "constitui o crime de fotografias ilícitas (Artigo 199.º do Código Penal), a realização de cópias informáticas de fotografias livremente acessíveis no Facebook e o seu envio posterior por email, por ter sido feita contra a vontade de quem elas retratavam. O facto de as fotografias estarem livremente acessíveis no Facebook não confere qualquer legitimidade para fazer cópias informáticas das mesmas e enviá-las por email, contra a vontade de quem elas retratavam."

Por fim, pode ainda fazer-se referência à Lei fundamental, como demonstra Simas (2014), a criminalidade informática está ligada à questão dos cidadãos exercerem livremente as suas liberdades e verem os seus direitos respeitados, como previsto na Constituição da República Portuguesa (CRP), no seu artigo 35.º, prevendo a "proteção das pessoas contra o tratamento de dados pessoais, atendendo à proibição de tratamento de determinados dados pessoais, assim como o direito de acesso aos dados que se encontrem em registos informáticos."

Não obstante, poderiam ser realçados mais diplomas legais, em particular direcionados à proteção de bases de dados e programas de computador, o cerne para o enquadramento foi referenciado dada a temática em apreço, na medida de danos e agressões a pessoas.

1.2.3. Estruturas nacionais de "combate" ao cibercrime

Em matéria de cibersegurança nacional podem encontrar-se algumas estruturas que desenvolvem atividades, passivas e ativas, no âmbito do cibercrime. Mas importa destacar as que oficialmente poderão ter uma intervenção direta na perssecução da responsabilidade criminal, nomeadamente: o Centro Nacional de Cibersegurança; o Gabinete Cibercrime da Procuradoria-Geral da República; e a Unidade Nacional de Combate ao Cibercrime e Criminalidade Técnológica da Policia Judiciária.

1.2.3.1. Centro Nacional de Cibersegurança (CNCS)

De acordo com a sua página oficial[6], "O Centro Nacional de Cibersegurança procura que o país use o ciberespaço de uma forma livre, confiável e segura, através da melhoria da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes, bem como da implementação das medidas e instrumentos necessários à antecipação, à deteção, à reação e recuperação de situações que, face à iminência ou ocorrência de incidentes ou ciberataques, ponham em causa o funcionamento das infraestruturas críticas e os interesses nacionais".

O CNCS tem ainda a obrigação de cooperação com as estruturas responsáveis pela ciberespionagem, ciberdefesa, ciberterrorismo, e em especial com o cibercrime, devendo comunicar à Polícia Judiciária os factos relativos à preparação e execução de crimes de que tenha conhecimento.

1.2.3.2. Gabinete Cibercrime da Procuradoria-Geral da República[7]

O Gabinete Cibercrime depende diretamente e tem sede na Procuradoria-Geral da República, podendo denominar-se também Gabinete de Coordenação da Atividade do Ministério Público na área da Cibercriminalidade.

Criado por Despacho do Procurador-Geral da República, a 7 de dezembro de 2011, este gabinete tem como principal objetivo "a coordenação interna, do Ministério Público, em tal área da criminalidade, a formação específica nesta matéria e o genérico estabelecimento de canais de comunicação com fornecedores de serviço de acesso às redes de comunicação, que permitam facilitar a sua colaboração na investigação criminal."[8]

É o próprio Ministério Público que realça a difícil compreensão judiciária do cibercrime, levando à necessidade de criar, aprofundar, consolidar e sedimentar entendimentos quanto às diversas problemáticas jurídicas

[6] *In* https://www.cncs.gov.pt/sobre-nos/missao-e-competencias/. Consultado em 30dec18.
[7] *In* http://cibercrime.ministeriopublico.pt. Consultado em 31dec18.
[8] *In* http://cibercrime.ministeriopublico.pt/pagina/o-que-fazemos-0. Consultado em 31dec18.

É nesse sentido que o Gabinete Cibercrime procura a coordenação, a formação específica de magistrados do Ministério Público, a interação com o setor privado e os órgãos de polícia criminal.

1.2.3.3. Unidade Nacional de Combate ao Cibercrime e Criminalidade Tecnológica (UNC3T) da Polícia Judiciária

Com o objetivo de promover o desenvolvimento de uma estratégia adequada de combate ao cibercrime, o Estado Português, através do Decreto-Lei n.º 81/2016 de 28 de novembro, veio referir que as entidades responsáveis pela prevenção e repressão devem deter informação (*cyber -intelligence*) em tempo útil que permita a deteção precoce de ataques digitais, a compreensão das intenções criminosas, bem como a comercialização e a disseminação de programas maliciosos. Nesse sentido, foi criada a UNC3T, uma unidade operacional e especializada da Polícia Judiciária, com o objetivo de procurar uma resposta estrutural, preventiva e repressiva do cibercrime.

As principais competências[9] da UNC3T visam a prevenção, deteção, investigação criminal e coadjuvação das autoridades judiciárias relativamente aos crimes previstos na Lei do Cibercrime; aos crimes praticados com recurso ou por meio de tecnologias ou de meios informáticos, previstos na Lei de Proteção de Dados Pessoais e no Código dos Direitos de Autor e Direitos Conexos. Tem ainda como responsabilidade a prevenção, deteção, investigação criminal e coadjuvação das autoridades judiciárias quanto aos crimes contra a liberdade e autodeterminação sexual, sempre que praticados por meio ou através de sistemas informáticos; de devassa por meio da informática; de burla informática e nas comunicações; relativos à interferência e manipulação ilegítima de meios de pagamento eletrónicos e virtuais; e de espionagem.

Importa referir que, decorrente da Lei de Organização da Investigação Criminal (LOIC)[10], é da competência reservada da Polícia Judiciária a investigação dos crimes informáticos e praticados com recurso a tecnologia informática, sem

[9] *In* https://www.policiajudiciaria.pt/unc3t/. Consultado em 31dec18.
[10] Art.º 7.º, n.º 3, al. l e Art.º 8.º da Lei n.º 49/2008 de 27 de agosto.

prejuízo de poderem ser deferidos a outro órgão de polícia criminal desde que tal se afigure, em concreto, mais adequado ao bom andamento da investigação.

1.3. *Cyberbullying*

1.3.1. Caracterização

A tendência crescente de interação e de práticas sociais no ciberespaço, contribuíram para o aumento de fenómenos como *cyberbullying*. Em Portugal é uma realidade a considerar, tratando-se de um fenómeno que parece ganhar contornos significativos, onde raparigas constituem a maioria das cibervítimas e rapazes a maioria dos *cyberbullies* (Cruz, 2011).

A maioria dos estudos e publicações consideram o cyberbullying como um novo comportamento de "*bullying*", enquadrando da mesma forma uma conduta intencional, repetitiva e prejudicial, numa relação caracterizada pelo desequilíbrio de poder entre agressor e vítima, mas com características diferentes e face à potencialidade das TIC.

O *bullying* carateriza-se por ser um comportamento de violência física, verbal ou emocional, com intenção, que é repetido ao longo do tempo e com abuso de poder entre os pares. Neste caso, a vitimização é uma conduta de agressão física e/ou psicológica realizada por um ou vários agressores contra uma vítima, através de uma ação intencionada, negativa e repetida, que coloca as vítimas numa posição frágil e sem condições de saída (Olweus, 1993 cit. por Ferreira, 2018).

De acordo com Neto (2005), pode classificar-se o *bullying* como direto ou indireto. O *bullying* direto traduz-se em agressões físicas, ameaças, roubos, ofensas verbais ou expressões e gestos que geram mal-estar nas vítimas. São atos mais frequentes em jovens do sexo masculino. Por sua vez, o *bullying* indireto compreende atitudes de negação, indiferença, isolamento, difamação, comportamentos mais frequentes em crianças e jovens do sexo feminino.

Em relação ao *cyberbullying* , este pode definir-se como um ato agressivo e intencional, realizado por um ou vários indivíduos, usando meios eletrónicos de comunicação, repetidamente e ao longo do tempo contra uma vítima que não se pode defender facilmente (Smith et al., 2008).

Seixas, Fernandes e Morais (2016, p. 21) reforçam o conceito, afirmando que "o *cyberbullying* constitui uma agressão intencional, por parte de um sujeito ou grupo de sujeitos, utilizando ferramentas/formas eletrónicas de contacto, repetidas vezes, para deliberadamente agredir, perseguir, intimidar, ameaçar, humilhar alguém que não se consegue defender facilmente. Ou, dito de outra forma, tem sido definido como o uso de tecnologias digitais a fim de se envolver de forma repetida em comportamento hostil, maldoso e agressivo que intencionalmente magoe ou prejudique outra(s) pessoa(s)."

Viegas (2017), realça que através das TIC têm-se promovido agressões verbais, contribuindo para a exclusão e isolamento social das vítimas, por força de divulgação de informação negativa ou falsa. Estes comportamentos antissociais enquadram práticas de *cyberbullying*, em que o agressor volta a agredir para intimidar, conquistar ou consolidar o domínio ou o poder sobre a vítima. Na prática, estes comportamentos podem mesmo vir a ser extremamente graves, dada a possibilidade de serem identificados numa fase adiantada da agressão. A título de exemplo, mas com contornos mais específicos, os recentes fenómenos denominados por "jogo da Baleia Azul" e "Momo", que incitavam à automutilação, violência e suicídio, bem como ao facto de terem associados roubos de informação pessoal e extorsão, onde as vítimas só foram detetadas após infligirem dados pessoais, como a automutilação ou mesmo tentativas de suicídio.

Para além da gravidade das agressões, existem mais variáveis subjacentes, uma vez que as agressões podem difundir-se facilmente e com enorme rapidez, mantendo-se infinitamente no ciberespaço. Um e-mail ou uma mensagem podem ser sucessivamente encaminhados para milhares de cibernautas, uma imagem, uma vez colocada em qualquer rede social, além de copiada e multiplicada, pode ficar eternamente no mundo virtual (Amado, Matos, Pessoa e Jäger, 2009).

A sensação de liberdade proporcionada pelo anonimato e invisibilidade, a instantaneidade, a facilidade de transmissão de mensagens e a falsa crença de impunidade, tendem a criar nos agressores a ideia de que podem praticar determinado tipo de comportamentos agressivos sem qualquer consequência (Garcez, 2014 cit. por Figueiredo e Matos, 2017).

Para Seixas et al. (2016), a desinibição criada pelo ciberespaço faz relegar princípios e valores, reconhecimento do dano provocado noutra pessoa, embaraço por condutas socialmente desaprovadas, bem como da perceção de uma possível ausência de consequências fruto do aparente anonimato sentido neste ambiente. Para os mesmos autores, o *cyberbullying* compreende ainda um conjunto de propriedades técnicas, nomeadamente: a persistência dos conteúdos digitais no ciberespaço, tudo aquilo que é publicado online fica na internet; a replicabilidade, a partir do momento em que se publique algo online esses conteúdos deixam de ter controlo; a escalabilidade, após uma publicação existe um enorme potencial da sua visibilidade; a pesquisabilidade dos conteúdos publicados; e as audiências desconhecidas que poderão ter acesso a esses conteúdos.

O *cyberbullying* tem uma maior prevalência na adolescência, não só pela maior autonomia e habilidade para utilizarem as TIC, mas também pela maior potencialidade de socialização. De acordo com Seixas et al. (2016, p. 66) verifica-se "uma tendência de aumento dos níveis de incidência até ao secundário (atingindo um pico por volta dos 14 anos/9º ano de escolaridade, aproximadamente), com estabilização ou descida progressiva a partir dos 15 anos."

Segundo um estudo[11] realizado no Reino Unido em relação ao *cyberbullying* nas redes sociais, 42% dos jovens vitimados na internet foram através do Instagram, 37% através o Facebook e 31%, pelo Snapchat. O Facebook já foi a plataforma mais usada para *cyberbullying*, chegando em 2013, a reunir 87% dos adolescentes vítimas de agressões virtuais. De acordo com o relatório da *Ditch The Label*, instituição internacional anti-*bullying*, "as formas mais comuns de ciberbullying incluem comentários desagradáveis publicados em perfis e fotos, mensagens privadas indesejadas e a criação de perfis falsos usando a imagem e informações da vítima" (Américo, 2017)[12].

[11] *In* https://olhardigital.com.br/noticia/facebook-nao-e-mais-a-rede-social-mais-usada-para-ciberbullying/69837. Publicação de Juliana Américo (19/07/2017, 16H50). Consultado em 03nov18.
[12] *In* https://olhardigital.com.br/noticia/facebook-nao-e-mais-a-rede-social-mais-usada-para-ciberbullying/69837. Publicação de Juliana Américo (19/07/2017, 16H50). Consultado em 03nov18.

1.3.2. Causas motivadoras

Os *cyberbullies*, segundo Pinheiro (2009), podem ser enquadrados em dois tipos; os acidentais e os adictos. Em relação aos *cyberbullies* acidentais, estes procuram gozar com a vítima ou retaliar como vingança. Para o efeito, usam perfis falsos, partilham imagens íntimas de alguém, são exibidas histórias, entre outros. Os casos de vingança por fim de namoro são frequentes nesta situação. Mas o que destaca este tipo de *cyberbullying* é o facto dos agressores não terem noção do efeito das suas ações sobre a vítima. Por sua vez, os *cyberbullies* adictos apresentam um comportamento bem mais grave, na medida em que as agressões praticadas proporcionam-lhes prazer. Até podem ter iniciado as agressões por acaso, mas ao sentirem prazer pela prática, começam a torná-la um hábito.

Num estudo desenvolvido por Montalvão (2015, p. 78), pode verificar-se que os agressores alegaram a prática de comportamentos de *cyberbullying* como "resposta a determinadas mensagens que receberam ou por algo que viram na internet" e que os levou a esse impulso, ou mesmo por brincadeira, dado que pensavam que seria divertido.

A jusante das causas verifica-se que o *cyberbullying* é hoje um problema comum entre crianças e jovens, em que estas agressões virtuais acabam por ter um impacto negativo na saúde física e mental das vítimas. Contudo, importa referir um elemento fulcral neste tipo de comportamentos, nomeadamente a intencionalidade de "agredir" o outro. Ficando claro que as situações de agressão que surgem em contextos inopinados e inesperados não se enquadram no fenómeno em apreço.

1.3.3. Enquadramento legal

Como já abordado anteriormente, Antunes e Rodrigues (2018) referem que os crimes praticados no ciberespaço denominam-se de cibercrimes, podendo ser realizados com recurso a redes digitais e às TIC.

O caso do *cyberbullying* poderá assim ser enquadrado como cibercrime, nos casos em que é desenvolvido através um conjunto de atividades ilícitas praticadas contra pessoas, mediante a utilização de redes digitais e TIC.

Apesar de não existir legislação específica que tipifique o *cyberbullying*, os comportamentos que caracterizam esta prática estão previstos e penalizados pelo ordenamento jurídico nacional. Desde a Constituição da República Portuguesa, ao Código Penal Português, à Lei do Cibercrime, a outros diplomas legais nacionais, bem como a orientações e determinações europeias, pode encontrar-se um regime sancionatório que tenta responder a estes casos e mostrar vontade de prevenção e repressão deste fenómeno.

Nesse sentido, também o Gabinete Cibercrime da Procuradoria-Geral da República, através de uma publicação[13] no seu site, procurou esclarecer que algumas atitudes e comportamentos são crime e que daí podem ser vítimas crianças e jovens. Não obstante, em sintonia com os diferentes Órgãos de Polícia Criminal (OPC), realça-se o direito à queixa criminal e os seus trâmites, bem como para a existência de uma resposta processual para a defesa dos direitos das vítimas do uso ilícito da internet.

Contudo, as disposições legais existentes não têm evitado esta prática e os consequentes danos nas vítimas. Está-se assim perante um ambiente digital sem o adequado controlo, onde se invocam muitos direitos e liberdades, onde muito ainda se consegue fazer sem o devido sentimento de estado de direito.

Não obstante, a atual política criminal nacional[14], determina orientações para uma prevenção e investigação prioritária em relação à cibercriminalidade e aos crimes praticados contra crianças e jovens. Da mesma forma, a norma em apreço determina que é prioritário a proteção da vítima e o ressarcimento dos danos por ela sofridos, em resultado da prática de crime, devendo ser-lhe facultados a informação e o apoio adequados à satisfação dos seus direitos.

1.3.4. Atores envolvidos

O fenómeno do *cyberbullying* apresenta vários intervenientes, dos quais se destacam os três principais atores, agressor, vítima e espectadores/observadores.

[13] TU E A INTERNET (AB)USO, CRIME E DENÚNCIA, Texto do Gabinete Cibercrime da Procuradoria-Geral da República. *In* http://www.ministeriopublico.pt/ebook/tu-e-internet. Consultado em 04nov19.
[14] Lei n.º 96 de 2017, de 23 de agosto.

Del Barrio (2013) cit. por Pessoa e Amado (2014), conclui que as vítimas são crianças e jovens menos populares, que sofrem problemas emocionais com os seus pares e possuem um conhecimento inadequado dos riscos e regras do uso seguro da internet (privacidade, *pass-words*, pedidos de ajuda, etc.). Por sua vez, os agressores caracterizam-se por ausência de empatia, confiança e segurança no uso das novas tecnologias, bem como perceção da falta de confiança, carinho e ajuda nas suas amizades.

Os mesmos autores abordam ainda o outro papel que tem sido identificado no desenvolvimento deste fenómeno, os observadores, que podem ser: apoiantes do agressor, podendo mesmo divulgar conteúdos agressivos, ampliando assim as agressões e o número de conhecedores; defensores da vítima; e testemunhas, estas com um papel passivo, que nem apoiam o agressor nem a vítima.

No entanto, importa realçar que, por vezes, existe uma troca de papéis entre vítima e agressor, movidos por sentimentos de vingança, aliado ao poder que as TIC garantem, não sendo necessário força nem presença física para perpetrar qualquer agressão virtual.

1.3.5. Tipos de comportamentos de *cyberbullying* e consequências da prática

Segundo Willard (2005) cit. por Montalvão (2015), podem considerar-se oito tipos de comportamentos que enquadram a prática de *cyberbullying*:

- *Flaming* - Envio de mensagens indelicadas e com raiva para uma pessoa ou grupo, no sentido de a lesar social e psicologicamente, bem como exercer autoridade sobre a mesma;
- *Harassment* - Assédio online, mediante o envio repetido a alguém de mensagens insultuosas e ofensivas;
- *Denigration* - Difamar alguém no ciberespaço através do envio ou da publicação de rumores sobre essa pessoa no sentido de lesar a sua reputação;
- *Impersonation* - Representação de alguém, fazendo passar-se por outra pessoa e enviar ou publicar conteúdos a fim de prejudicá-la;

- *Outing* - Divulgação de informação sensível, privada, constrangedora ou de imagens privadas;
- *Trickery* – Falar com alguém online a fim de lhe obter informação pessoal através de engano, para posteriormente divulgá-la;
- *Exclusion* - Excluir alguém de um grupo online intencionalmente e de forma cruel;
- *Cyberstalking* - Perseguição on-line, assédio repetido e intenso a fim de denegrir e provocar medo na vítima. As redes sociais têm permitido aos stalkers obter mais facilmente informação sobre as vítimas.

Além destas formas de *cyberbullying*, Kowalski, Limber e Agatson (2012) cit por Montalvão (2015), acrescentaram mais duas:

- *Happy Slapping* - Com origem nas estações de metro de Inglaterra, caracteriza-se por grupos de jovens agredirem alguém e o incidente ser gravado por elementos do grupo através de telemóveis, para posteriormente ser publicado na internet e visualizado por inúmeras pessoas;
- *Sexting* - Envio ou divulgação de fotografias ou vídeos com conteúdos eróticos, sensuais e sexuais, com imagens pessoais, através de mensagens de texto ou de outros meios eletrónicos, com o objetivo de prejudicar alguém.

Tendo em conta a diversidade de comportamentos associados ao *cyberbullying* que têm vindo a ser desenvolvidos, Hinduja e Patchin (2015) cit. por Montalvão (2015), apresentaram ainda mais quatro formas:

- *Photoshopping* - Manipulação ou alteração de imagens no sentido de prejudicar a vítima ou colocá-la num contexto comprometedor ou embaraçoso;
- *Confession Pages* - Páginas na internet ou redes sociais que permitem aos utilizadores, de forma anónima, partilhar segredos ou outro tipo de confissão pessoal, mas que podem levar a comentários agressivos e que se enquadram no cyberbullying;
- *Tagging and Untagging* - A vítima sem o pretender, é identificada (tagged) ou conectada com uma determinada afirmação, imagem ou vídeo, fruto das conexões entre perfis online e determinados conteúdos nas redes sociais;

- *Physical threats* - Ameaças físicas, traduzem-se em ameaças à segurança física e ao bem-estar da vítima, merecendo especial atenção no sentido de verificar a sua credibilidade.

Tendo em consideração as diversas agressões de que poderão ser alvo, Field (2018), demonstra que a literatura recente apresenta várias consequências para as vítimas de *cyberbullying*, nomeadamente: predisposição e tentativas suicidas; sintomas psiquiátricos como depressão e ansiedade; abuso de substâncias psicoativas; sintomas somáticos, caracterizados por problemas físicos; angústia e frustração no desempenho de tarefas diárias, bem como no encontro de soluções para os problemas. Estes efeitos podem variar em função das agressões, género e faixa etária. Alguns estudos apontam mesmo a depressão e os comportamentos suicidas como dominantes entre os adolescentes.

Todas estas consequências acabam por influenciar significativamente a vida pessoal das vítimas. Além disso, especialistas "consideram que o impacto psicológico e emocional provocado pelo *cyberbullying* nas vítimas e nas suas famílias, traduzido em sentimentos de dor e sofrimento, de humilhação, raiva ou vulnerabilidade, podem também repercutir-se na escola" (Worthen, 2007 cit. por Figueiredo e Matos, 2017, p. 126).

1.3.6. Mecanismos de intervenção

"... após o início da partilha de uma foto ou de outro conteúdo que visa afetar psicologicamente a vítima, a primeira preocupação desta e das autoridades consiste em estancar a difusão. Para tal, a primeira ação consiste em tentar que o conteúdo seja retirado dos servidores do prestador do serviço da rede social." (Antunes e Rodrigues, 2018, p. 62).

Independentemente dos diferentes espaços e aplicações que permitem a vivência no ciberespaço, em especial as redes sociais, advertirem para a proibição de condutas criminais ou simplesmente ações contra a sua política de utilização, não tem sido possível impedir a prática de agressões virtuais e comportamentos antissociais entre os diferentes utilizadores.

Nesse sentido, entidades públicas e privadas têm procurado fazer face a este fenómeno com várias iniciativas e de diferentes abordagens.

Por recomendação[15] do Conselho da Europa, os Estados-Membros têm a obrigação de reconhecer a qualquer pessoa os direitos humanos e liberdades fundamentais no contexto da utilização da Internet. Sendo aplicáveis os instrumentos e convenções em matéria de cibercriminalidade e do direito à vida privada e proteção de dados pessoais. "Os direitos humanos, que são universais e indivisíveis, e as normas conexas têm primazia sobre os termos e condições gerais impostos aos utilizadores da Internet por qualquer agente do setor privado." (Recomendação CM/Rec (2014)6 do Comité de Ministros, p. 3).

A referida recomendação prevê que crianças ou jovens têm direito a proteção especial e orientação quando utilizam a Internet. Atribuindo-lhes o direito de se exprimir livremente, participarem na sociedade, receberem formação de professores, educadores e pais ou tutores sobre a utilização segura da Internet, incluindo sobre como preservar a sua privacidade.

A recomendação realça que crianças ou jovens devem ter presente que os conteúdos criados na Internet podem ficar acessíveis ao mundo inteiro e comprometer a sua dignidade, segurança e privacidade, e que a seu pedido, tais conteúdos devem ser eliminados ou suprimidos.

Da mesma forma, devem ser-lhes facultadas informações sobre conteúdos e comportamentos ilegais e a forma de os denunciar, procurando-se, assim, uma proteção especial contra ameaças, em especial contra as formas de cibercriminalidade.

Neste contexto, crianças ou jovens têm direito a um recurso efetivo sempre que os seus direitos e liberdades forem violados, permitindo-lhes obter uma reparação adequada. Esse recurso pode ser obtido junto dos prestadores de serviços de Internet, das autoridades públicas ou de instituições de direitos humanos.

---

[15] Recomendação CM/Rec(2014)6 do Comité de Ministros aos Estados-Membros sobre o Guia dos Direitos Humanos para os Utilizadores da Internet (Adotada pelo Comité de Ministros em 16 de abril de 2014, na 1197.ª reunião dos Delegados dos Ministros). *In* https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-cm-rec-2014-6-of-the-committee-of-ministers-to-member-states-on-a-guide-to-human-rights-for-internet-users-adopted-by-the-committee-of-?inheritRedirect=false. Consultado em 17nov18.

O "prestador de serviços de Internet, os fornecedores de acesso a conteúdos e serviços em linha ou outra empresa e/ou autoridade pública devem facultar-lhe informação sobre os seus direitos, liberdades e vias de recurso possíveis, e como usufruir dos mesmos, nomeadamente informação facilmente acessível sobre como denunciar e reclamar contra ingerências nos seus direitos, e como obter reparação pelas mesmas." (Recomendação CM/Rec (2014)6 do Comité de Ministros, p. 16).

Tem sido ao nível da sensibilização que são identificadas mais iniciativas, em particular em diferentes espaços na internet, considerando ainda os demais canais de denúncia e apoio para eventuais ocorrências. Para o efeito, destacam-se diversas linhas de apoio, como blogs e sites, onde são apresentadas explicações sobre o fenómeno e orientações para vítimas e agressores, pais, professores e demais envolvidos que possam ter intervenção na situação. Noutros casos vai-se mais além, realçam-se as formas de denúncia e os mecanismos de apoio à vítima, bem como os apoios telefónicos ou online para todos os potenciais envolvidos neste fenómeno.

Existem ainda referências da possibilidade de, perante a identificação de situações graves, as remeterem de imediato para as autoridades competentes. Da mesma forma, garantem ações de sensibilização a toda a comunidade e o envolvimento de diferentes entidades para intervenções mais especializadas.

Face ao exposto, tendo em consideração o panorama nacional, podem realçar-se alguns desses espaços que procuram dar uma resposta ao cyberbullying, nomeadamente, o Instituo de Apoio à Criança, Miúdos Seguros na Net, Associação Portuguesa de Apoio à Vítima, Centro de Internet Segura, Projeto Segurnet, Portal Bullying, Internet Segura, entre outros.

Dando especial evidência a um destes espaços para melhor caracterizar as suas ações, e dada a forma como aborda o assunto, bem como pela missão a que se propõe, destaca-se a Linha Alerta[16] que faz parte do projeto[17] Internet Segura[18]**.** Co-financiado pela Comissão Europeia, deste projeto fazem parte diversas entidades: a FCT – Fundação para a ciência e a Tecnologia; a Direcção-Geral do Ministério da

[16] *In* http://linhaalerta.internetsegura.pt/index.php. Consultado em 17nov18.
[17] (awareness node e linha de denúncia).
[18] *In* https://www.internetsegura.pt/. Consultado em 17nov18.

Educação; a Fundação Portugal Telecom; a Microsoft Portugal; e o IPDJ – Instituto Português do Desporto e Juventude.

Segundo a divulgação do projeto, este disponibiliza uma linha de denúncia[19] segura e confidencial, por meio de formulário Web, telefone ou email, onde o público em geral pode reportar potenciais conteúdos ilegais na Internet.

Esta "Linha Alerta" procura ajudar no bloqueio de conteúdos ilegais na Internet e que se consiga garantir o procedimento criminal contra os autores dessas publicações, nomeadamente de pornografia infantil, de apologia da violência e do racismo. Para o efeito, conta com as autoridades policiais a quem lhes reporta a informação das denúncias e com os *Internet Service Providers* (ISP) nacionais para a rápida remoção desses conteúdos.

Também as autoridades policiais têm formas rápidas de denúncia para estes casos, mediante os contactos telefónicos disponíveis ou mesmo pela queixa eletrónica existente nas suas páginas *online*.

1.3.6.1. Prevenção do cyberbullying

"Prevenir a ocorrência do cyberbullying requer uma estratégia conjunta e articulada entre os professores, os pais, os estudantes e os diversos elementos da comunidade" (Montalvão 2015, p. 36).

A formação de professores, funcionários, alunos e pais sobre *cyberbullying* é fundamental para se conhecer e prevenir. As escolas devem solicitar apoio de autoridades públicas e privadas para partilharem conhecimento sobre o fenómeno, formas de prevenção e intervenção, bem como sobre práticas seguras de utilização da internet e assim envolver todos os intervenientes que poderão ter um papel ativo na sua prevenção.

As crianças e jovens devem saber refletir antes de qualquer publicação na internet, deixando a emoção de parte e as urgências de resposta, para que possam ter ponderação das suas ações (Hinduja & Patchin, 2015) cit. por Montalvão (2015).

[19] Mantida pela Fundação para a Ciência e a Tecnologia (FCT) e pelo seu serviço de resposta a incidentes de segurança informática da Rede Ciência, Tecnologia e Sociedade – RCTS CERT.

Devem ainda "ser devidamente informados das consequências legais que este fenómeno acarreta, bem como do impacto que o *cyberbullying* causa a terceiros" (Willard, 2005) cit. por (Montalvão 2015, p. 37).

De referir que, entre 2008 e 2010, foi desenvolvido um trabalho internacional apoiado pela Comunidade Europeia, no sentido de desenvolver um manual para formadores sobre *cyberbullying*, suportado numa investigação desenvolvida por especialistas, investigadores e pelos próprios formadores. Desse trabalho nasceu o projeto europeu *CyberTraining: A Research-based Training Manual On Cyberbullying*.

Com este manual foi possível constituir um conhecimento mais aprofundado do problema e, por outro lado, garantir programas de formação para os diferentes intervenientes, proceder a diagnósticos e possibilitar intervenções nas diferentes situações. Constitui-se assim como um instrumento essencialmente prático, que procurou dar resposta às dificuldades dos formadores, bem como divulgar orientações para uma maior prevenção do fenómeno de *cyberbullying* (Matos, A., Pessoa, T., Amado, J. e Jäger, T., 2011).

1.3.6.2. Estudos científicos para intervenção no *cyberbullying*

O fenómeno do *cyberbullying* tem despertado interesse na comunidade científica, a qual tem dado a conhecer uma série de trabalhos desenvolvidos nesta área. Por forma a conhecer-se o que estudos científicos têm concluído, irão abordar-se alguns deles, que analisam e dão a conhecer formas de intervir neste fenómeno.

1.3.6.2.1. "Fuzzy Based Genetic Operators for Cyber Bullying Detection Using Social Network Data".

Deviet (2018), apresenta um artigo onde aborda o problema da deteção do *cyberbullying* a partir de texto. Nesse projeto foi desenvolvido um codificador automático, nomeadamente um mecanismo que procura a identificação de agressores e vítimas através da deteção de mensagens nas redes sociais, utilizando algoritmos e a respetiva análise dos dados criados nessas redes. Para o efeito, foram criados filtros

que procuram palavras-chave e a sua consequente incorporação, através de conjunto de técnicas de modelagem de linguagem e de aprendizagem no processamento da linguagem, em que palavras ou frases do vocabulário são mapeadas.

1.3.6.2.2. "A Machine Learning Approach for Detecting Aggressive tweets in Spanish".

Este estudo efetuado por Gómez-Adorno, H., Bel-Enguix, G., Sierra, G., Sanchez, O. e Quezada, D. (2018), começa por dizer que devido ao aumento do cyberbullying contra os utilizadores das redes sociais, a deteção automática destas agressões começou a chamar a atenção. A deteção de agressões através de texto é o primeiro passo para identificar automaticamente o *cyberbullying*. Desta forma, o artigo em apreço apresenta um estudo para detetar tweets agressivos em espanhol, conseguindo identificar 42,85% de expressões agressivas, o que lhe permitiu alcançar o 5º. lugar numa análise com outros 12 sistemas participantes.

1.3.6.2.3. "Content-Driven Detection of Cyberbullying on the Instagram Social Network".

Haoti Zhong, H.L., Squicciarini, A., Rajtmajer, S., Griffin, C., Miller, D. e Caragea, C. (2016), apresentaram numa conferência internacional sobre Inteligência Artificial, a possibilidade de deteção do *cyberbullying* em redes sociais de partilha de fotos, mediante o desenvolvimento de mecanismos de alerta para a previsão de imagens partilhadas, suscetíveis ou vulneráveis a ataques. De acordo com o conteúdo partilhado, os autores investigaram o uso de imagens e legendas para uma deteção aperfeiçoada do *bullying*. O estudo foi validado através de um conjunto de dados com mais de 3.000 imagens, juntamente com os comentários efetuados na rede social Instagram.

A perceção das características do conteúdo partilhado pode revelar-se extremamente útil para o desenvolvimento dos mecanismos de alerta a fim de prevenir o *bullying*. Neste trabalho foram desenvolvidos métodos para detetar o *cyberbullying* em comentários após a publicação de imagens no Instagram.

Aproveitando as características das imagens e legendas colocadas, utilizando os instrumentos desenvolvidos foi possível classificar os comentários que contêm *bullying* com mais de 93% de precisão.

1.3.6.2.4. "Abused Word Detection on Social Media".

Este artigo publicado num jornal internacional, aborda um algoritmo de correspondência de palavras, que procura identificar mais rapidamente as que se tornam abusivas/agressivas e ocultá-las da área de divulgação pública, no sentido de garantir um ambiente social mais saudável nas redes sociais. Para esse fim, na análise de dados, procura-se examinar os comentários de cada utilizador, procurando as palavras abusivas para aumentar o número dessas palavras no conjunto de dados. Desta forma, identifica-se a agressividade do utilizador e o nível de assédio existente nas redes sociais. Contudo, os diferentes tipos de palavras não são detetados pelo algoritmo.

Face aos diferentes tipos de idiomas, com os diferentes tipos de palavras abusivas/agressivas e com diferentes erros de redação, torna-se realmente difícil reconhecer a palavra que é o foco do problema. Facto que torna o ambiente social poluído ou doentio para os jovens e que potencia um impacto negativo nas suas mentes. Foi com o objetivo de melhorar esse ambiente, que os autores deste artigo propuseram um sistema que esconde nas redes sociais as palavras abusivas/agressivas (Yenurkar, T., Nandurkar, A., Thute, N. e Shete, R., 2018).

1.3.6.2.5. "Aggression Identification Using Deep Learning and Data Augmentation".

Risch, J. e Krestel, R. (2018), referem que as plataformas das redes sociais, como o Facebook, o YouTube, o Twitter e o Instagram, permitem que milhões partilhem publicamente conteúdos, muitos de forma agressiva. Neste artigo, os autores consideraram o problema da identificação desses conteúdos agressivos publicados nessas redes sociais, apresentando para o efeito um sistema de identificação automática de tais publicações prejudiciais e/ou agressivas.

Para os autores essa identificação é importante, na medida em que pode moderar as discussões online. Além disso, a automatização permite análises sem precedentes de conjuntos de dados de discussão que contêm milhões de publicações.

1.3.6.2.6. "Police actions with regard to cyberbullying: The Belgian case."

Neste estudo, Vandebosch, H., Beirens, L., D'Haese, W., Wegge, D., e Pabian, S. (2012), começaram por realçar que, para além de estudantes, pais, escolas e fornecedores de serviços de Internet, a polícia foi também identificada como um ator importante nas diferentes abordagens contra o *cyberbullying*. Tendo em consideração a situação na Bélgica, este artigo descreve como a polícia pode intervir neste fenómeno criminal. Preventivamente, a polícia poderá informar e sensibilizar estudantes, pais e escolas sobre o assunto. Ao nível da deteção, realça-se a possibilidade de criar sistemas de denúncia e relatórios online; por fim, pode a polícia ajudar no tratamento dos casos existentes, identificando os autores das agressões e ajudando as vítimas.

Para continuar a abordagem ao *cyberbullying*, foi mencionado a existência de uma *Federal Computer Crime Unit (FCCU)*, que trabalha em estreita relação com as *Regional Computer Crime Units (RCCU)*. As principais tarefas destas Unidades de Crime Informático são combater crimes ao nível das TIC, como fraude na Internet, *hacking*, espionagem e sabotagem; bem como, efetuar investigações forenses sobre as TIC usadas para outros crimes e fornecer apoio para investigações na Internet. A FCCU também efetua a gestão de uma linha direta na Internet, a www.ecops.be, onde os utilizadores podem denunciar crimes perpetrados no ciberespaço.

É possível verificar neste artigo que lidar com crimes como *cyberbullying* não é estritamente limitado a um nível policial. Embora os cidadãos possam usar a linha direta da FCCU para denunciar situações de *cyberbullying*, apenas em casos específicos é que realmente se torna numa tarefa da FCCU ou das RCCU.

A polícia local é considerada o primeiro ponto de contato para a maioria das situações de *cyberbullying*. No entanto, a polícia local nem sempre tem o adequado conhecimento para lidar com esses casos, solicitando, desta forma, apoio da FCCU e

das RCCU. Esta estrutura de intervenção policial de diferentes níveis, torna-se bastante complicada e pode criar confusão nos cidadãos aquando da necessidade de efetuarem as denúncias.

Face à sua importância, importa realçar as principais tarefas que a polícia pode realizar face ao *cyberbullying*, nomeadamente: prevenção com base no conhecimento do fenómeno; deteção e receção de denúncias; e por fim, parar o crime, identificar o agressor e ajudar a vítima, em particular removendo os conteúdos nocivos e agressivos.

Nesta dinâmica é realçado que ambos os níveis policiais estão envolvidos nas diferentes tarefas, bem como estas são muitas vezes desenvolvidas em cooperação com outros parceiros, como as escolas, os ISP e o sector de segurança eletrónica.

Ao lidar com casos de *cyberbullying*, a polícia local, com a ajuda das RCCU ou, em casos muito sérios, da FCCU, procurará identificar o autor, contando com os dados fornecidos pela vítima, como os registros da agressão: datas, horários e locais virtuais, conteúdo da(s) mensagens, nomes de utilizador, endereços de e-mail, entre outros. A partir desses dados, a polícia geralmente tem ainda de solicitar a colaboração dos ISP e dos sites que permitem a ligação do agressor com a vítima, principalmente as redes sociais.

Para concluir, o artigo realça a importância de efetuar uma abordagem integrada ao *cyberbullying*, envolvendo jovens, pais, escolas, polícia e ISP. Os pais, as escolas e as organizações de segurança eletrónica podem educar para a vivência online, ensinando os jovens a terem comportamentos seguros e apropriados. Podem ainda monitorar de perto as atividades online dos seus filhos e alunos, bem como intervir em determinados casos, por exemplo, solicitando a um autor conhecido que elimine o conteúdo prejudicial, ou denunciando um abuso por um desconhecido aos ISP.

O envolvimento da polícia é necessário nos casos em que o *cyberbullying* representa uma séria ameaça à saúde mental e/ou física da vítima, e é necessária uma cooperação rápida com ISP para identificar o infrator e impedir o crime. No entanto, esta dinâmica requer melhores procedimentos internacionais para obter os vestígios digitais, princípios de retenção para todos os ISP, procedimentos adequados de

"notificação e remoção" e mais "polícia cibernética", não se envolvendo apenas em análise forense de Tecnologias de Informação.

1.4. Responsabilidade dos *Internet Service Providers* (ISP)

"*Os fornecedores de serviços, tais como os administradores de páginas web, de redes sociais (...) devem assegurar uma utilização segura e responsável dos seus serviços através da implementação de mecanismos de filtragem, da disponibilização de ferramentas que possibilitem o relato e o registo de casos de uso inapropriado ou de cyberbullying, de forma a apoiar as culturas de auto-regulação dos utilizadores e, ainda, aumentando a cooperação entre empresas e com a autoridades."* (Amado, Matos, Pessoa e Jäger, 2009, p. 319).

1.4.1. Prestadores de serviço de acesso à internet

De forma geral, em Portugal os ISP são considerados organizações que garantem aos utilizadores o acesso à internet. Segundo a Autoridade Nacional de Comunicações (ANACOM)[20], entidade reguladora do sector das comunicações, o serviço de acesso à internet pode ser disponibilizado através de diversas tecnologias e é oferecido com várias capacidades de transmissão que se traduzem na prestação de serviços de banda estreita ou banda larga.

Considerando o Dec. Lei n.º 7/2004, de 07 de janeiro[21], com a sua versão mais recente atribuída pela Lei n.º 46/2012, de 29 de agosto, houve uma transposição para a ordem jurídica interna de Diretivas do Parlamento Europeu e do Conselho, relativo a aspetos legais dos serviços da sociedade de informação, do tratamento de dados pessoais e da proteção da privacidade no sector das comunicações eletrónicas.

Perante o diploma em apreço, verifica-se que não existe uma responsabilidade direta dos ISP no controlo do tipo de informação e conteúdos que circulam nos seus servidores. Contudo, importa realçar o instituído pelo art.º 13.º daquele diploma, nomeadamente os deveres dos ISP, cabendo-lhes a obrigação para com as entidades

[20] *In* https://www.anacom.pt/render.jsp?contentId=430538. Consultado em 31dec18.
[21] Lei do Comércio Eletrónico no Mercado Interno e Tratamento de Dados Pessoais.

competentes de: informar quando tiverem conhecimento de atividades ilícitas desenvolvidas através dos seus serviços; identificar os destinatários dos serviços com quem tenham acordos de armazenagem; prevenir ou pôr termo a uma infração, removendo ou impossibilitando o acesso a informação; e ainda, de fornecer listas de titulares de sítios que alberguem, quando lhes for pedido.

Não havendo obrigatoriedade de controlo da informação que circula, existe o dever de impedir práticas ilícitas, removendo conteúdos danosos e impossibilitando o seu acesso aquando do seu conhecimento.

Mais recentemente foi a ordem jurídica reforçada com o Regulamento Geral de Proteção de Dados[22], que, independentemente de todas as orientações, prevê a licitude do tratamento de dados pessoais quando for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento, desde que esse tratamento respeite a essência dos direitos e liberdades fundamentais e constitua uma medida necessária e proporcionada para assegurar a segurança pública, a prevenção, a investigação, a deteção ou a repressão de infrações penais.

1.4.2. Prestadores de serviço de Redes Sociais

No âmbito internacional e considerando a prestação de serviço que efetuam, as redes sociais também são consideradas ISP. Para Antunes e Rodrigues (2018), atualmente as redes sociais são as aplicações que mais contribuem para a pegada digital dos utilizadores da internet. Com o fim de desenvolver relações sociais no ambiente digital e a partilha de conteúdos com outros utilizadores, existe também a tendência de partilha de conteúdos desapropriados que contribuem negativamente para a pegada digital dos seus autores.

No entanto, e de forma a contribuir para um ambiente digital mais saudável, as redes sociais permitem que os seus utilizadores denunciem publicações abusivas ou mesmo ilegais, assim como, estas tendem a monitorizar conteúdos públicos que

[22] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

possam violar as condições de utilização, levando à remoção dos mesmos e à eventual exclusão dos infratores.

Fazendo uma abordagem às redes sociais mais utilizadas por crianças e jovens, procurar-se-á efetuar uma pequena observação da sua preocupação para com o *cyberbullying*, dado que são um dos potenciadores do fenómeno.

No Facebook[23] pode verificar-se a intenção de criar uma ideologia de segurança na utilização da rede social. Através do seu Centro de Segurança, existe a preocupação em desenvolver políticas, ferramentas e recursos para que as pessoas se sintam mais seguras aquando da sua utilização. Procuram criar um ambiente seguro para todos, criando regras sobre o que se pode partilhar, formas para as pessoas controlarem os conteúdos que partilham, bem como a disponibilização de manuais com orientações sobre partilha de conteúdos e as respetivas consequências para os próprios e terceiros, fazendo uma clara abordagem à prevenção do *cyberbullying*. No sentido de impedir este fenómeno, existe mesmo um Centro de Prevenção de *Bullying*, constituindo-se como "um recurso para adolescentes, pais e educadores à procura de apoio e ajuda para problemas relacionados com o *bullying* e outros conflitos. Oferece planos passo a passo que incluem indicações de como iniciar algumas conversas importantes para pessoas que sofrem de bullying, pais que têm um filho a sofrer ou a ser acusado de *bullying* e educadores que têm alunos envolvidos em *bullying*."

Mas é o próprio Facebook que realça a necessidade de trabalhar com agentes de autoridades para promover a segurança *online* e *offline*. Levando por vezes à necessidade de fornecer informação para responder a emergências, em especial as que envolvem o risco imediato de danos físicos, a prevenção de suicídios e à recuperação de crianças desaparecidas. Da mesma forma, podem ainda fornecer informação para impedir ou responder a situações de fraude ou outra atividade ilegal, assim como os incumprimentos dos Termos do Facebook.

No sentido de operacionalizar esta coordenação, existem para os agentes de autoridade as normas para as autoridades responsáveis pela aplicação da Lei, que regulam a procura de registos do Facebook e do Instagram. Contudo, a divulgação

[23] *In* https://www.facebook.com/safety/groups/law/guidelines/. Consultado em 03nov18.

de registos de contas terá de estar de acordo com os termos de serviço e a legislação aplicável[24], podendo ser necessário um pedido de Acordo sobre Auxílio Judiciário Mútuo ou uma carta rogatória para forçar a divulgação dos conteúdos de uma conta. Para este fim podem ser enviados pedidos formais de preservação de dados através do Sistema de Pedidos *Online* para Autoridades ou por *e-mail*, garantindo posteriormente o envio de informações sobre o processo legal em curso.

Para situações que carecem de uma resposta imediata, nomeadamente as que envolvem "perigo iminente para uma criança ou o risco de morte ou de ferimentos graves para qualquer pessoa e quando é necessária a divulgação de informações sem demoras, um agente da autoridade pode enviar um pedido através do Sistema de Pedidos *Online* para Autoridades."[25]

Também os utilizadores podem obter os conteúdos da sua conta, como mensagens, fotos, vídeos e publicações na cronologia, basta que acedam à funcionalidade que lhes permite descarregar a sua informação a partir das respetivas definições de conta.

No caso do Instagram[26], a empresa procura também assumir o combate ao *bullying*, neste caso ao *cyberbullying*, levando a que as pessoas se sintam confortáveis para se expressar, mas também seguras e apoiadas quando necessário. Para o efeito, tem vários conselhos na aplicação para reagir a situações de qualquer abuso virtual, passando inicialmente por bloquear e deixar de seguir a pessoa que está agindo abusivamente. Contudo, se a situação prevalecer, poderá usar ferramentas de denúncia diretamente para os gestores da aplicação.

De acordo com um artigo *online*[27], o porta-voz da rede social mencionou que os utilizadores podem "desativar comentários ou fazer a sua própria lista de palavras

[24] "É necessário um mandado de busca emitido em conformidade com os procedimentos descritos nas *Federal Rules of Criminal Procedure* (Regras Federais do Processo Penal) ou com procedimentos de mandado estaduais equivalentes, após a demonstração de causa provável, para forçar a divulgação dos conteúdos armazenados de qualquer conta, que podem incluir mensagens, fotos, vídeos, publicações na cronologia e informações de localização." *In* https://pt-pt.facebook.com/safety/groups/law/guidelines/. Consultado em 26nov18.

[25] *In* https://pt-pt.facebook.com/safety/groups/law/guidelines/. Consultado em 26nov18.

[26] *In*https://help.instagram.com/426700567389543/?helpref=hc_fnav&bc[0]=Ajuda%20do%20Instagram&bc[1]=Centro%20de%20Privacidade%20e%20Seguran%C3%A7a. Consultado em 26nov18.

[27] *In* https://olhardigital.com.br/noticia/facebook-nao-e-mais-a-rede-social-mais-usada-para-ciberbullying/69837. Consultado em 26nov18.

e *emojis*[28] que desejam banir dos seus comentários." Da mesma forma, através do desenvolvimento tecnológico, estão a testar aplicações para que comentários ofensivos sejam automaticamente bloqueados e não apareçam nas contas das pessoas." Para além do já referido, os utilizadores são ainda encorajados a denunciar a violência através das ferramentas de denúncia da própria rede social.

Por sua vez, a rede social Snapchat[29] para partilha de momentos, para além de incentivar a denúncia de casos de *bullying*, disponibiliza informação sobre o fenómeno, recursos e ajuda adicional aos *Snapchatters*, pelo menos nos Estados Unidos, através de uma linha de apoio para uma solução colaborativa do problema, mediante apoio emocional através de conselheiros treinados.

Em relação ao WhatsApp[30], o *bullying* pode assumir várias formas dado que é um serviço de mensagens, muitas vezes abusivas quando em grupo. Para que a vítima se possa proteger, deverá bloquear e excluir determinados contactos. De acordo com a empresa, para situações fora de controlo, deverá ser enviado um e-mail para mais informações sobre a problemática.

Mediante *tweets* ou respostas indesejadas, bem como quaisquer outros abusos, poderá deixar de seguir ou bloquear esse utilizador e denunciá-lo diretamente para o Twitter[31], existindo para o efeito páginas de conselhos que podem ajudar. A empresa tem ainda parceiros espalhados pelo mundo a fim de ajudarem localmente os utilizadores que necessitam de garantir procedimentos de segurança.

Por fim o Youtube[32] defende a sua utilização sem medo de ser sujeito a qualquer intimidação ou assédio. Realçando que os abusos devem ser denunciados e os conteúdos publicados analisados, no sentido de verificar se existe incumprimento dos termos de uso para a consequente remoção dos mesmos. A empresa defende que quando detetados conteúdos "maliciosos", deverão ser utilizadas as ferramentas de denúncia adequadas para que o autor seja ainda eliminado.

---

[28] "Símbolo gráfico, ideograma ou sequência de caracteres [ex.: :-), :-(, ^_^] que expressa uma emoção, uma atitude ou um estado de espírito, geralmente usado na comunicação eletrónica informal". *In* https://dicionario.priberam.org/emoji. Consultado em 31jul19.

[29] *In* https://www.snap.com/pt-PT/safety/safety-center/. Consultado em 27nov18.

[30] https://www.whatsapp.com/security/. Consultado em 27nov18.

[31] https://about.twitter.com/pt/safety.html. Consultado em 27nov18.

[32] https://support.google.com/youtube/answer/2802268?hl=pt&ref_topic=2803176. Consultado em 27nov18.

2. METODOLOGIA

2.1. Abordagem metodológica e modelo de Análise

A aquisição de conhecimento prevê um conjunto de formalismos associados à investigação. Considerando os diferentes métodos de investigação científica, aplicou-se no presente trabalho o método dedutivo. Proposto por Aristóteles (384 a.C. - 322 a.C.), "baseia-se num raciocínio racional e lógico, que parte do geral para o particular." (Sarmento 2013, p. 8).

Através deste raciocínio dedutivo, partiu-se de teorias para uma realidade particular, ou seja, a partir de investigações, abordagens teóricas e reflexões sobre o problema, procurou-se uma verdade.

Independentemente da sua subjetividade, a investigação em causa baseou-se numa estratégia qualitativa no sentido de obter a informação necessária. A partir de valores, crenças e opiniões, é possível alcançar um entendimento sobre o objeto de estudo, atribuindo significados a partir de padrões encontrados nos dados recolhidos. (Vilelas, 2009).

A adoção de uma abordagem qualitativa permitiu reunir estudos, reflexões e conhecimentos de especialistas na matéria, que contribuíram preponderantemente para se atingir os objetivos propostos neste trabalho, possibilitando a compreensão do fenómeno em estudo e as suas necessidades de intervenção.

O processo de investigação em apreço desenvolveu-se através de um modelo de análise que teve por base as questões de investigação formuladas, a Pergunta de Partida e as Derivadas desta, que acabam por assumir a dinâmica do processo.

Assim, formulou-se a seguinte PP - Qual a resposta imediata que as vítimas de *cyberbullying* necessitam?

Derivadas da PP e no sentido de contribuir para a sua resposta, formularam-se as seguintes PD:

PD 1 - De que forma poderão ser cessadas as agressões virtuais de *cyberbullying*?

PD 2 - De que forma poderão ser identificados os autores de agressões virtuais de *cyberbullying*?

PD 3 - Quais os mecanismos para obter prova das agressões virtuais de *cyberbullying*?

PD 4 - Quais as ações a serem tomadas para apoiar as vítimas de agressões virtuais de *cyberbullying*?

Com base nas PD e no corpo de conhecimento analisado, procurou-se atingir os OE definidos, nomeadamente:

OE1 - Descrever como se poderão cessar as agressões virtuais de *cyberbullying*;

OE2 - Descrever como se poderão identificar os autores de agressões virtuais de *cyberbullying*;

OE3 – Identificar os mecanismos para recolher e preservar a prova digital de agressões virtuais de *cyberbullying*;

OE4 - Identificar as ações que poderão ser tomadas para apoiar as vítimas de agressões virtuais de *cyberbullying*.

Com o alcançar dos OE foi possível concretizar o OG, identificando e caracterizando a primeira resposta às vítimas de *cyberbullying*, no sentido de procurar uma maior proteção da vítima e minimizar os efeitos da agressão.

2.2. Procedimentos de investigação

O trabalho em apreço reuniu três principais fases do processo de investigação (Sarmento, 2013, p. 11), a fase exploratória, a fase analítica e a fase conclusiva.

Na fase exploratória, a análise da conjuntura atual através de publicações sobre o tema, levou à sua delimitação e à identificação do problema da investigação, que se refletiu a partir das questões de investigação formuladas. Delimitado o tema, seguiu-se uma revisão da literatura existente, de trabalhos e investigações desenvolvidas, bem como de notícias que enquadram o problema. Assim, foi possível averiguar o estado atual do conhecimento sobre o fenómeno em apreço, do contexto do ciberespaço e quais as iniciativas se têm desenvolvido para fazer face ao *cyberbullying*. Para além de conceitos e teorias, foram ainda analisadas investigações

científicas desenvolvidas para combater este flagelo, que também permitiram reunir resultados sobre a temática.

A fase analítica teve como objetivo a recolha, o registo e o tratamento de mais dados, e iniciou-se com a conceção do guião da entrevista. Este guião, que define o inquérito por entrevista semiestruturada aplicado, baseou-se na análise exploratória da primeira fase metodológica e nos objetivos da investigação. Este instrumento de recolha de dados é constituído por oito (8) perguntas (conforme Apêndice A) e foi testado em dois especialistas, que trabalham operacionalmente na área, com o objetivo de validar a forma como as questões foram concebidas, a clareza dos termos e conceitos utilizados, e a compreensão geral do tema.

Seguidamente, foi aplicado individualmente o inquérito por entrevista semiestruturada, ou semidiretiva, previamente validada, a um conjunto de especialistas na área de estudo, permitindo reunir informação e conhecimento existente a partir de diferentes pontos de vista.

Os dados do inquérito por entrevista foram obtidos diretamente com os especialistas. Foi efetuado um contacto prévio, com o objetivo de, por um lado, explicitar o estudo em questão e o porquê de ter sido considerado para este e, por outro, procurar obter a sua autorização e a forma para a realização da mesma. Preferencialmente procurou-se realizar as entrevistas presencialmente, mas devido a fatores temporais e espaciais, em alguns casos optou-se pela realização da entrevista através do envio por meios eletrónicos (*e-mail*). Em cada *e-mail* enviado encontrava-se uma carta de apresentação, que enquadrou a natureza do projeto e os objetivos pretendidos, conforme Apêndice B. A recolha destes dados decorreu durante o mês de março e abril de 2019.

Posteriormente, as respostas à entrevista foram objeto de uma análise de conteúdo mediante uma observação qualitativa dos dados obtidos, que, depois de analisadas e confrontadas com o enquadramento teórico do trabalho, foi possível o desenvolvimento das conclusões. De acordo com Quivy e Campenhoudt (2008), o método da entrevista, seguida da análise do seu conteúdo, é dos métodos que mais se utilizam, permitindo uma investigação aprofundada e com um grau de validade satisfatório.

No paradigma qualitativo, deve haver uma preocupação com a qualidade dos dados e proceder para que estes reflitam a perspetiva do interveniente e do grupo de especialistas. Assim, a fase de tratamento e interpretação dos dados obtidos seguiu o postulado de que a importância de um registo, e do seu conteúdo, aumenta com a frequência da sua aparição.

Para finalizar, a fase conclusiva permitiu atingir os objetivos estabelecidos a partir da obtenção das respostas às questões derivadas da PP e, por conseguinte, responder à PP.

Seguiu-se a discussão de resultados obtidos e a apresentação de reflexões e descobertas (Sarmento, 2013), que permitiram um contributo para o conhecimento e a idealização de uma nova resposta ao *cyberbullying*.

3. APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

Decorrente da investigação proposta, o inquérito por entrevista foi o procedimento adotado na recolha de dados e esclarecimentos junto de especialistas reconhecidos e experientes na área de estudo, o que levou ao apuramento de conhecimentos preponderantes para se atingir os objetivos propostos.

No presente capítulo efetuar-se-á a apresentação e análise dos resultados obtidos através das entrevistas. Para o efeito, serão apresentados os excertos das respostas dos entrevistados, permitindo desta forma, após análise e sistematização das mesmas, identificar as suas ideias principais e a frequência dos seus principais argumentos. De forma a possibilitar uma melhor compreensão das respostas extraídas, bem como o seu alcance, cada questão formulada na entrevista será apresentada individualmente.

Seguidamente as respostas serão objeto de uma análise de conteúdo, mediante a observação qualitativa desses dados e o consequente cruzamento com a informação reunida no enquadramento teórico.

Questão n.º 1

Face à particularidade do *cyberbullying*, de que forma poderiam ser cessadas as agressões virtuais e minimizados os seus efeitos nas vítimas?

A presente questão procurou identificar formas ou processos para terminar com as agressões virtuais que constituem o *cyberbullying*, ou mesmo mecanismos para cessar uma agressão quando identificada, permitindo diminuir as suas consequências nas vítimas.

Tendo em conta a prespectiva da questão, parte dos entrevistados (E1, E4 e E6) realçam a importância do desenvolvimento de mecanismos tecnológicos para que automáticamente se consiga efetuar o controlo, o bloqueio, ou mesmo a remoção, de conteúdos e comunicações que enquadrem este tipo de violência. Ideias que corroboram com alguns estudos analisados anteriormente, como Deviet (2018), que desenvolveu um mecanismo automático que procura a identificação de agressores e vítimas através da deteção de mensagens nas redes sociais, utilizando algoritmos e a

respetiva análise dos dados criados nessas redes. Também como Adorno, Enguix, Sierra, Sanchez e Quezada (2018), que face ao aumento do *cyberbullying* contra os utilizadores das redes sociais, procuraram a deteção automática destas agressões, realçando que a deteção através de texto é o primeiro passo para identificar automaticamente o *cyberbullying*. Assim como, Zhong, Li, Squicciarini, Rajtmajer, Griffin, Miller e Caragea (2016), que nos apresentaram a possibilidade de deteção do *cyberbullying* em redes sociais de partilha de fotos, mediante o desenvolvimento de mecanismos de alerta para a previsão de imagens partilhadas, suscetíveis ou vulneráveis a ataques.

Já a maioria dos entrevistados entende ser importante a melhoria dos processos e mecanismos de reporte e denúncia entre todos os intervenientes, podendo passar pela criação de canais de comunicação e ajuda em tempo real, com a respectiva intervenção de especialistas (E1, E3, E4, E5 e E7). Para este efeito, também a plataforma Youtube defende a utilização das ferramentas adequadas para a denúncia dos conteúdos abusivos e a sua posterior análise, no sentido de verificar se existe incumprimento dos termos de uso que levem à consequente remoção dos mesmos, bem como à eliminação dos seus autores.

Existindo os crimes necessários para sancionamento destes comportamentos, foi abordado pelos E6 e E7 a importância da existência e aplicação da Lei a fim de garantir o seu efeito. Também a educação pessoal e para as tecnologias, bem como a sensibilização para o fenómeno, poderá evitar que agressores reincidam e se contribua para que as vítimas superem das agressões sofridas, conforme realçado pelos E2 e E6. Torna-se cada vez mais importante um conhecimento alargado destas matérias, até mesmo para que as potenciais vítimas se consigam proteger, bloqueando e excluindo do seu circuito eventuais agressores.

No entanto, o E2 alerta que, a difusão massificada das redes sociais e das diferentes plataformas comunicação, potenciaram o desenvolvimento das ligações em qualquer momento, levando a que este tipo de agressões se tornassem mais fáceis. Factos que levaram o ainda o E2, mas também os E3 e E5, a abordar a dificuldade em cessar este tipo de agressões.

Entrevistado	Conteúdo
E1	- (…) envolvimento dos ISP (…) através do controlo automático de conteúdos nas redes sociais e com a criação de "linhas" ou facilidades de ajuda às vítimas em tempo real, as quais pudessem contar com especialistas que para além da ajuda imediata tivessem a capacidade de apoiar a vítima em situação "pós-traumática".
E2	- (…) não se perspetiva que este tipo de manifestação venha a cessar (…). A expansão total das redes de comunicação e dos aparelhos de comunicações, bem como a difusão massificada das redes sociais potenciam a comunicação a todo o momento, entre pessoas que estão sempre "ligadas" e contactáveis (…). - (…) o assédio e a agressão à distância tornam-se muito mais fáceis. Somente por via de educação pessoal e para as tecnologias se pode evitar que agressores reincidam e se pode contribuir para que as vítimas superem as agressões.
E3	- Dificilmente se conseguirá por força do género humano. - - (…) melhoria dos mecanismos de reporte, de queixa e de remoção (…) quando percebamos que existe um abuso é necessário que mais gente o marque e o reporte.
E4	- Pelo bloqueio, remoção, inibição e comunicação proativa e automatizada (quando possível) das publicações e comunicações que se enquadram neste fenómeno (…). - Este tipo de ações terão de ser acompanhadas por processos de comunicação expeditos entre todos os intervenientes (autoridades, comunidade, ISP, plataformas de social media) para uma atuação articulada das autoridades e de entidades que prestem apoio a vítimas (…).
E5	- (…) dificilmente as agressões virtuais no ciberespaço cessarão. - (…) todos os esforços que possam minimizar essa "agressão" têm de ser desenvolvidos e postos em prática.
E6	- O importante é a sensibilização (…). - Do ponto de vista legal julgo que não há muito mais a fazer, a não ser uma mão pesada aquando da aplicação da Lei, dado que os crimes necessários para sancionarem estes comportamentos já existem (ameaças, injúrias, entre outros). - (…) é possível também em termos tecnológicos criar filtros para que se bloqueiem atividades desta natureza, no entanto sendo difícil fazê-lo porque estas podem circular em mensagens privadas.
E7	- (…) qualquer medida de proteção terá de partir de uma denúncia (…). - Para serem cessadas as agressões será necessário legalmente estar previsto que quando denunciada uma situação de cyberbullying, os ISP, deverão retirar e arquivar a informação relacionada com as agressões.

Quadro n.º 1 - Resumo das respostas à questão n.º 1 da Entrevista

Questão n.º 2

Como poderão os *Internet Service Providers* (ISP) (redes sociais, *links*, plataformas de *e-mail*) procurar o bloqueio, rastreabilidade e remoção dos conteúdos ilícitos no ciberespaço?

A questão em apreço procurou identificar como poderiam os ISP eliminar conteúdos ilicitos no ciberespaço, em particular os que enquadram agressões virtuais.

Perante as respostas foi identificada a possibilidade de rastreabilidade e bloqueio de conteúdos definidos como ilícitos e lesivos para as vítimas (E2, E3, E4, E6 e E7).

No entanto a maioria dos entrevistados começou por abordar uma actuação proactiva. Mediante o emprego de meios técnicos, foi realçada a importância do controlo automático e a sinalização de conteúdos suspeitos ou que se revelem uma

ameaça, lançamento de alertas para o ofendido e agressor, conjugando a situação e esclarecendo as consequências (E1, E2, E3, E4 e E7). No caso da rede social Instagram, os utilizadores podem desativar comentários ou fazer a sua própria lista de palavras e *emojis* que desejam banir dos seus comentários, além de se encontrarem a desenvolver aplicações para que comentários ofensivos sejam automaticamente bloqueados e não apareçam nas contas dos utilizadores.

Foi realçado por alguns entrevistados a possível censurabilidade na remoção de determinados conteúdos, daí a necessidade de perceber o contexto e o tipo de conteúdo em causa para que seja possível atuar mediante os formalismos legais e processuais em vigor. O E2 aborda o facto de estar em discussão no Parlamento Europeu a responsabilização dos ISP pela remoção conteúdos ilícitos e os constrangimentos dessa atuação.

Segundo o E5, o problema ainda é ao nível legal, visto que esses conteúdos, ou "ação ilegal", não podem ser removidos ou eliminados de imediato pelos ISP, dado que existem procedimentos processuais para essa remoção, podendo o aspeto temporal da justiça levar tempo à sua concretização.

No entanto o E6 refere que no caso das redes sociais a situação é diferente, quando existem mensagens abertas ou em áreas públicas, com conteúdos que se enquadram no *cyberbullying*, pode-se aplicar as regras que existem, em particular o Dec. Lei 7/2004, que trata da Lei do Comércio Eletrónico, que permite e em determinados casos impõe, que os prestadores de serviços de comunicações, que fazem armazenagem de conteúdos, bloqueiem os que são considerados ilícitos. Este entrevistado vai mais longe, no caso das redes sociais, afirma que se justifica criar um regime de alguma responsabilização pelos conteúdos que são fornecidos por terceiros, mas que acabam por ser disponibilizados a outros terceiros por via das suas plataformas. Finaliza realçando que, por denúncia, os ISP têm a obrigação de intervir face à evidência de conteúdos ilícitos.

Perspetiva também reforçada pelo E2, que refere que os alojadores de conteúdos podem, por iniciativa própria ou por solicitação das autoridades públicas, remover ou bloquear conteúdos, de acordo com os respetivos critérios. Podendo apenas surgir dificuldade de articulação pelo facto da maioria estar baseada fora de Portugal.

Para o E3 e E7, perante a denúncia de conteúdos e a confirmação da sua ilegalidade, os ISP deveriam removê-los, guardando os dados e metadados das comunicações para a prossecução criminal.

Por sua vez, o E6 salienta que as mensagens privadas que contenham conteúdos ilícitos não podem ser bloqueadas ou removidas. De momento, apenas as mensagens abertas ou numa área pública podem ser removidas, e mediante uma notificação prévia ou denúncia. Contudo, este entrevistado realçou a procura de desresponsabilização das redes sociais, em particular por disponibilizarem "um serviço, em que há um fornecimento de conteúdos propriamente dito, só que estes prestadores alegam que os conteúdos não são disponibilizados pelo próprio, eles apenas disponibilizam a plataforma e que terceiros, os *Users*, *User Generated Content* (UGC), é que lá disponibilizam os conteúdos, e aí é que existe grande questões porque estes prestadores de serviço não são ISP propriamente ditos. Contudo, são estes prestadores que têm maior responsabilidade nos conteúdos que circulam."

Por fim, o E4 destaca a importância e consciencialização da denúncia deste fenómeno às autoridades, independentemente do bloqueio e remoção dos conteúdos ilícitos, bem como, da salvaguarda pelos ISP e fornecedores de plataformas de social media dos registos necessários.

Em linha com o racional dos entrevistados, tem-se a nível nacional o projeto Internet Segura[33], que detém uma Linha Alerta[34] para o público em geral denunciar, de forma segura e confidencial, potenciais conteúdos ilegais na Internet. O objetivo passa por ajudar no bloqueio desses conteúdos ilegais e garantir o procedimento criminal contra os autores dessas publicações. Para o efeito, reporta às autoridades policiais a informação das denúncias e conta com os ISP nacionais para a rápida remoção desses conteúdos. No entanto, o efeito de uma intervenção imediata poderá perder-se com o empenhamento de vários intervenientes, nomeadamente o apoio e encaminhamento das vítimas, e todas as medidas ao alcance dos OPC, nacionais e internacionais.

[33] *In* https://www.internetsegura.pt/.
[34] *In* http://linhaalerta.internetsegura.pt/index.php.

Entrevistado	Conteúdo
E1	- O controlo de conteúdos automático é tecnicamente possível (…) é possível rastrear conteúdos previamente definidos como ameaça, instar o seu autor a justificar ou remover (…)
E2	- (…) tecnicamente, é possível aos fornecedores de serviços bloquear conteúdos que identifiquem como agressivos ou lesivos. - (…) tema principal do célebre Artigo 13, um projeto legislativo ainda aberto, em discussão no Parlamento Europeu, no qual está em causa saber: (i) se os ISP devem poder ter a iniciativa e o dever de retirar os conteúdos, havendo consequências se não retirarem ou (ii) se a ordem deve ser sempre de uma autoridade pública (que é o que acontece agora), ou ainda (iii) se é legítimo que ISPs, que são privados, exerçam competências de autoridades públicas (e ainda se é legítimo que tenham o custo necessário, que passa por uma estrutura de vigilância sistemática das redes). - Nada impede os alojadores de conteúdos de, por iniciativa própria ou por sugestão das autoridades públicas, remover ou tornar inacessíveis determinados conteúdos. Porém, como a maior parte dos alojadores de conteúdos está baseada fora de Portugal, na prática, não é fácil a articulação com os mesmos. Resta comunicar-lhes a existência de determinados conteúdos e esperar que, segundo os respetivos critérios, em sede de autorregulação, os removam.
E3	- (…) estas plataformas (…) podiam apostar mais em meios técnicos para sinalização de suspeição e posterior confirmação. Perante a queixa e a confirmação, deveriam remover, mas guardar os dados e os metadados das comunicações associadas por período limitado de tempo para fins de prossecução criminal.
E4	- Isto implica atuar não apenas em função de uma denúncia, mas também proactivamente (…) - Independentemente da ação de bloqueio e remoção de conteúdos, é importante a consciência e sentido de responsabilidade social para a denúncia às autoridades sobre este tipo de atividade, independentemente da formalização de uma denúncia pela vítima. Nesse aspeto os ISP e fornecedores de plataformas de social media podem e devem ter a iniciativa de salvaguardar os registos e, proactivamente, agir em defesa da vítima.
E5	- Apesar de ser censurável e de se saber que determinada ação "ilegal" está presente ela não poderá ser removida ou eliminada de imediato seja por quem a disponibiliza (o prestador do serviço) ou transporta (o operador de serviço). - (…) o problema não é técnico, mas sim legal. O procedimento processual para que o(s) conteúdo(s) seja(m) removido(s) existe, mas o aspeto temporal da justiça pode ser dilatado no tempo.
E6	- (…) as mensagens privadas não podem ser bloqueadas ou removidas. Agora em redes sociais, com mensagens abertas ou numa área publica, em que existam mensagens de cyberbullying é diferente, já se pode aplicar as regras que existem, em particular o Dec. Lei 7/2004, que trata da Lei do comércio eletrónico, que permite e em determinados casos impõe, que os prestadores de serviços de comunicações, que fazem armazenagem de conteúdos, bloqueiem conteúdos ilícitos. - (…) eles não têm obrigação de vigiar a rede e os conteúdos que circulam através dos seus serviços, mas se forem avisados que circulam conteúdos ilícitos, aí eles têm obrigação de bloquear, tem que haver uma notificação prévia. - (…) um serviço como o youtube ou facebook, que têm umas plataformas, em que disponibilizam um serviço, em que há um fornecimento de conteúdos propriamente dito, só que estes prestadores alegam que os conteúdos não são disponibilizados pelo próprio, eles apenas disponibilizam a plataforma e que terceiros, os users, user generated content (UGC), é que lá disponibilizam os conteúdos, e aí é que existe grande questões porque estes prestadores de serviço não são ISP propriamente ditos. Contudo, são estes prestadores que têm maior responsabilidade nos conteúdos que circulam. - (…) justifica-se criar-lhes um regime de alguma responsabilização pelos conteúdos que são fornecidos por terceiros, mas que acabam por ser disponibilizados a outros terceiros por via das suas plataformas. - Por denúncia têm a obrigação de operar quando os conteúdos forem manifestamente ilícitos, ainda mais quando são os próprios a colocar lá os conteúdos.
E7	- (…) os ISP apenas deverão atuar com um processo de bloqueio quando existir uma denúncia.

	- O ISP quando detetar situações de eventual agressão deveria automaticamente lançar um alerta para o agressor e para o agredido, realçando que tal comportamento poderá enquadrar algum tipo de crime e quais as consequências e procedimentos.

Quadro n.º 2 - Resumo das respostas à questão n.º 2 da Entrevista

Questão n.º 3

Quais os mecanismos técnicos e legais que poderão possibilitar a identificação dos autores de *cyberbullying*?

A presente questão procurou mostrar mecanismos que levem à identificação dos autores de *cyberbullying*.

A identificação dos agressores, como nos demais crimes, é de extrema importância, não só para que se faça justiça, mas principalmente para garantir a sua recuperação e impedir que continuem este tipo de prática. Como referido por Garcez (2014) cit. por Figueiredo e Matos (2017), o *cyberbullying* proporciona uma sensação de liberdade dada pelo anonimato e invisibilidade, bem como pela instantaneidade e facilidade na transmissão de mensagens, levando a uma falsa crença de impunidade que tende a criar nos agressores a ideia de que podem praticar as suas agressões virtuais sem consequências.

O E1 começa por falar do controlo de conteúdos e identificação da origem dos dados. Tendo em conta as normas legais, os responsáveis pelas plataformas de comunicação podem implementar "heurística e alarmística" a fim de identificar a origem dos dados que retratem uma ameaça. Já o E3 fala numa ação oficiosa de identificação para as autoridades em caso de deteção do *cyberbullying* e a reação de bloqueio perante uma queixa.

Por sua vez, grande parte dos entrevistados abordam a questão direcionando-a para os mecanismos definidos no ordenamento jurídico, com a respetiva envolvência das autoridades competentes. O E2 realça que já existem mecanismos legais suficientes para no âmbito das investigações obter esses registos, nomeadamente devido às regras de retenção e preservação de dados das comunicações e posteriormente a sua entrega às entidades policiais e judiciárias. O E6 refere mesmo que os mecanismos existentes são os aplicáveis à maioria dos crimes informáticos ou cibercrimes. Conforme a Lei do Cibercrime, os OPC podem de imediato pedir a guarda e conservação dos dados ao prestador de serviço de comunicações eletrónicas, e caso este não tenha os dados necessários, qual a entidade

que os poderá ter. Segundo o E6, os OPC podem de imediato pedir a conservação dos dados, enquanto que a junção ao processo, em determinados casos, terá de ser por pedido do Ministério Público ou Juiz de Instrução. No entanto, o E3 refere ainda a possibilidade de adoção de normas legais que contribuam para um acesso mais rápido e fiável, pelas autoridades judiciárias ou policiais, a metadados de comunicações de suspeitos. Por fim, o E7 vem reforçar a necessidade dos ISP conservarem e disponibilizarem a informação quando solicitada pelas autoridades competentes, enfatizando a necessidade de criação de procedimentos próprios para garantir o acesso rápido, a fim de garantir a persecução da justiça.

O E4 vai mais longe e realça a importância de adoção de todos os mecanismos que permitam preservar e recolher evidências, desde os dados do utilizador, local e equipamentos utilizados e pela correlação dos registos recolhidos pelos intervenientes nas comunicações/publicações, por forma a reconstruir com exatidão todo o percurso e detalhes da comunicação, "desde o utilizador – plataforma de *social media* – ISP – vítima".

Não obstante, foi possível identificar uma perfectiva diferente. O E5 refere que os intervenientes nesta matéria possuem o *knowhow* suficiente para coadjuvar as autoridades judiciais no combate ao *cyberbullying*, sendo necessário que todos funcionem de forma eficiente e em complemento na sua área de atuação.

Entrevistado	Conteúdo
E1	- (…) técnicas de controlo de conteúdos e identificação de origem dos dados, são atualmente vulgares quer nas plataformas de redes sociais, quer nos sistemas de proteção como IDS/IPS, bastará que os ISPs responsáveis pela disponibilidade das facilidades de comunicação implementem heurística e alarmística adequada à identificação da origem dos dados que consubstanciam a ameaça de acordo com as normas legais em vigor (…)
E2	- (…) na Internet tudo fica registado e Portugal tem na sua legislação mecanismos suficientes permitir às investigações criminais obter esses registos. Portugal tem regras de retenção de dados de comunicações, normas que permitem que as mesmas se preservem e que venham a ser facultadas às entidades policiais e judiciárias.
E3	- (…) ação oficiosa em caso de deteção, e a reação (bloqueio) perante queixa, deveriam estar entre as primeiras formas de possível ação. - (…) a inclusão ou a adesão a um sistema do tipo "Cloud Act" (Clarifying Lawful Overseas Use of Data) poderia contribuir para um acesso mais rápido e fiável a metadados de comunicações de suspeitos (…) que obrigará sempre a intervenção das autoridades judiciárias ou de polícias em quem seja delegado esse contacto.
E4	- (…) todos aqueles que permitem a preservação e recolha de evidências que permitam essa identificação. Passará necessariamente de recolher todos os detalhes possíveis do utilizador, local e equipamentos utilizados e pela correlação dos registos recolhidos pelos intervenientes nas comunicações/publicações, por forma a reconstruir com exatidão todo o percurso e detalhes da comunicação, desde o utilizador – plataforma de social media – ISP – vítima.

E5	- Os técnicos dos operadores e prestadores do serviço de comunicações eletrónicas, da academia, civil e militar, reguladores e autoridades policiais possuem o know how suficiente para coadjuvar as autoridades judiciais no combate ao cyberbullying. Para que ele seja eficaz todos terão de funcionar de forma eficiente, e em complemento, na sua área de atuação.
E6	- Os mecanismos são os existentes para a maioria dos crimes informáticos ou cibercrimes (…), sempre que haja conhecimento da prática do crime (…) não pode ser o próprio a atuar dado que não irá obter muita informação, pode até tirar print screens e armazenar informação que tenha ao seu dispor e possa visualizar, mas não melhor do que ter a informação fornecida pelos ISP, estes sim têm informações muito úteis e podem ter acesso ao terceiro que foi colocar os conteúdos nas suas plataformas e terem os endereços IP que mais tarde poderão ser úteis para saber quem foi a pessoa responsável por essa colocação. - Os OPC estão limitados áquilo que podem fazer, o quadro legal está delimitado na Lei do Cibercrime, estes podem pedir logo a guarda e conservação dos dados e podem inclusivamente pedir ao prestador de serviço de comunicações eletrónicas se tem os dados necessários, e se não qual a entidade que ele acha que poderá ter esses dados. - Os OPC podem logo pedir a conservação, não podem é pedir a junção. Em determinados casos, em que é necessário dados de tráfego ou os endereços de IP, terá muitas vezes de ser por pedido do MP ou Juiz de Instrução.
E7	- Os ISP deverão ser obrigadas a conservar e disponibilizar, a informação, quando solicitado pelas autoridades judiciais competentes, devendo ser identificados procedimentos próprios para garantir o acesso rápido de forma a garantir a eficiência e eficácia da ação da justiça.

Quadro n.º 3 - Resumo das respostas à questão n.º 3 da Entrevista

Questão n.º 4

De que forma poderão os ISP (redes sociais, *links*, plataformas de *e-mail*) colaborar com as autoridades policiais na identificação do perfil ou conta dos autores do *cyberbullying*?

Com esta questão pretendeu-se conhecer formas de colaboração dos ISP na identificação do perfil ou conta dos autores do *cyberbullying*.

Todos os entrevistados direcionaram as suas respostas para a importância da criação de canais ou pontos de contacto para que se consiga uma comunicação imediata e aquisição da informação necessária de forma célere. Para o efeito, seria necessário oficializar uma colaboração entre as diferentes entidades envolvidas, a fim de se conseguir uma resposta rápida e eficaz a na resolução deste tipo de incidentes. O E1 realça ainda a importância de existirem especialistas em ambas as partes para o tratamento deste fenómeno.

Contudo, a maioria dos entrevistados particulariza a necessidade dos ISP preservarem os dados relevantes e os divulgarem rapidamente às autoridades policiais (E1, E2, E3, E4, E6 e E7). O E4 enfatiza ainda a necessidade desses dados para de "forma célere e eficaz atuar junto da vítima (proteção) e junto do autor (prossecução criminal)". Atuação que, conforme o E6, deverá ser de acordo com o Código Processo Penal e a Lei do Cibercrime.

Não obstante, também a Recomendação CM/Rec (2014)6 do Comité de Ministros previu que os ISP, os fornecedores de acesso a conteúdos e serviços em linha e as autoridades públicas devem colaborar nesta matéria, no sentido de facultar às vítimas informação sobre os seus direitos, liberdades, vias de recurso e denúncia possíveis, assim como obter a reparação dos seus direitos.

Entrevistado	Conteúdo
E1	- Com a criação de canais céleres, pontos de contacto únicos e protocolos de colaboração efetivos que permitam uma primeira resposta rápida e eficaz a este tipo de incidentes na rede, (…) bem como que existam especialistas de ambas as partes para o tratamento desta tipologia desviante.
E2	- A cooperação entre entidades privadas e públicas é crucial (…) sendo, portanto, essencial que estes mesmos privados possam (e devam) cooperar com as autoridades de justiça na investigação criminal.
E3	- Pontos de contato dedicados a Law Enforcement Agencies, remoção e salvaguarda de dados do abuso e dos metadados relacionados, entrega direta às polícias de investigação criminal. (…) por recurso a protocolos bilaterais, ou por harmonização legal, com legislação especial.
E4	- (…) assegurando que recolhem e preservam o maior detalhe possível de registos para que as autoridades policiais possam, de forma célere e eficaz atuar junto da vítima (proteção) e junto do autor (prossecução criminal) (…) é especialmente relevante a comunicação imediata, voluntária e detalhada, por qualquer ISP ou plataforma de social media, de qualquer indício de atividade de cyberbullying que tenham conhecimento através dos seus mecanismos de deteção.
E5	- Os eventuais protocolos existentes entre os prestadores de serviço e as autoridades judiciais deverão ser transversais a toda a temática cyber (cybercrime, cybersecurity, cyberbullying)
E6	- (…) eles têm que ser notificados pelas autoridades, - Só podem aceder, conservar ou fornecer esses dados de acordo com o Código Processo Penal e a Lei do Cibercrime, por regra eles só podem conservar e depois enviam diretamente às autoridades policiais. Mas têm essa obrigação de colaborar.
E7	- Disponibilizando a informação necessária de forma célere. - Apoiando campanhas de sensibilização. Através da divulgação de resultados de rastreamento - denúncia.

Quadro n.º 4 - Resumo das respostas à questão n.º 4 da Entrevista

Questão n.º 5

De que forma poderá ser obtida a prova digital das agressões virtuais efetuadas contra as vítimas de *cyberbullying*?

A presente questão procurou mostrar como será possível adquirir prova das ocorrências de *cyberbullying*.

A maioria dos entrevistados direcionou a sua resposta para a componente legal existente (E1, E2, E4, E5 e E7). Em particular, em sede de investigação criminal, a aplicação e cumprimento das regras jurídicas de preservação e obtenção de dados de comunicações. Nesta componente, o E7 ainda refere a importância de se estabelecerem protocolos interinstitucionais com a origem dos servidores para que se acelere a disponibilização da informação. A rede social Facebook facilita essa

disponibilização, mediante um pedido através do Sistema de Pedidos Online para Autoridades, desde que efetuado por agentes da autoridade.

O E1 refere que a prova "deve ser recolhida na sua origem, evitando adulteração da mesma", bem como, de acordo com legislação em vigor, que deverão os ISP (neste caso redes sociais) a garantir a sua preservação e interrupção da atividade criminosa. Situação reforçada pelo E6, que nos diz que até pode ser feito um *printscreen* e/ou captura de imagem pela vítima, mas melhor será pedir ao ISP de armazenagem (website ou Rede Social) para preservar e fornecer os conteúdos e endereços IP do cliente que lá colocou essa informação. A recolha de prova pelas vítimas pode ser adulterada, daí a importância das Forças de Segurança "solicitarem ao prestador de serviços de comunicações para armazenar esses conteúdos, e de maneira a saber quem é o infrator". Podem solicitar a conservação dos dados, a título e exemplo, tanto ao Facebook como à MEO, porque qualquer um deles tem prova. "Os ISP têm provas relativamente à identificação, o Facebook poderá não ter esses dados, mas tem prova dos conteúdos nocivos e ofensivos."

Tal como o E6, também Vandebosch, Beirens, D'Haese, Wegge e Pabian (2012), realçam a importância das Forças de Segurança (FS) intervirem no *cyberbullying*, nomeadamente na prevenção do fenómeno, na deteção e receção de denúncias, na cessação do crime, passando pela identificação do agressor e na ajuda da vítima, e em particular, removendo os conteúdos nocivos e agressivos. Mas importa ainda evoluir, esta intervenção policial requer melhores procedimentos internacionais para obter os vestígios digitais, princípios de retenção para todos os ISP, procedimentos adequados de "notificação e remoção" e mais "polícia cibernética", não se envolvendo apenas em análise forense de Tecnologias de Informação.

Por fim, o E3 e E5 abordam a componente técnica para a aquisição de prova do *cyberbullying*. Em que o E3 propõe o desenvolvimento de um mecanismo automático (tipo botão de pânico), através das plataformas de comunicação, para preservação da informação digital quando o utilizador detete qualquer conteúdo ilegal.

Entrevistado	Conteúdo
E1	- (…) basta a aplicação efetiva das regras internacionais de preservação de dados implementada nas plataformas de comunicações (…) em cumprimento das regras processuais penais ou outras aplicáveis, sempre com o patrocínio dos ISPs. - A prova digital (…) deve ser recolhida na sua origem, evitando adulteração da mesma (…) a vítima poderá indicar que elementos probatórios consubstanciam a agressão, mas será sempre do ISP (redes sociais) o ónus da preservação, que deverá também pugnar pela célere interrupção da atividade criminosa, em respeito pela legislação em vigor.
E2	- (…) é legal e operacionalmente possível obter, em sede de investigação criminal, dados de conteúdo de comunicações (…) e ainda os dados de identificação e localização de quem comunica.
E3	- A incorporação de um mecanismo semelhante ao "botão de pânico" que funcionasse automaticamente para salvaguarda de informação digital. O utilizador, ao ser surpreendido por informação adversa, carrega numa opção associada ao post em causa, e esse facto leva a que a plataforma, de uma só vez, guarde a informação relevante (…).
E4	- Sempre através dos meios de recolha de prova e de custódia da prova que é utilizado para qualquer investigação criminal no âmbito da criminalidade informática.
E5	- Esse é um assunto sensível cuja solução é técnica, mas onde não se pode esquecer, ou ultrapassar, a vertente jurídica. (…) o operador e o prestador de serviço de comunicações eletrónicas tem a facilidade tecnológica do seu lado, importa é apurar se juridicamente pode e/ou como deve fazer com autonomia.
E6	- Imaginando que teve lugar num web site aberto a todos, poderá ser feito um printscreen e capturar a imagem, só que nada melhor do que pedir depois ao ISP para guardar aqueles conteúdos, o ISP pode fazer isso, neste caso o ISP de armazenagem. - Aquele que armazena o website ou as páginas do Facebook, pode armazenar os conteúdos algum tempo para depois os fornecer, e depois deve guardar os endereços IP do cliente que lá colocou essa informação. - (…) se a vítima fizer um printscreen da agressão e enviar para a GNR ou Polícia pode ser facilmente alterado ou deturpado. Por isso nada melhor do que as Forças de Segurança solicitarem ao prestador de serviços de comunicações para armazenar esses conteúdos, e de maneira a saber quem é o infrator. - (…) é pedir desde logo que conserve o endereço IP daquele quadro de agressão. - O OPC pode solicitar a conservação dos dados, tanto ao Facebook como à MEO, porque qualquer um deles tem prova. Os ISP têm provas relativamente à identificação, o Facebook poderá não ter esses dados, mas tem prova dos conteúdos nocivos e ofensivos.
E7	- Considerando a localização dos servidores em países com políticas de privacidade e justiça distintas, terá de ser protocolado entre os Ministérios da Justiça impondo processos de trabalho e comunicação interinstitucional que acelerem a disponibilização da informação.

Quadro n.º 5 - Resumo das respostas à questão n.º 5 da Entrevista

Questão n.º 6

Quais as ações e em que momento, dentro e fora do ciberespaço, deverão ser desenvolvidas para minimizar os danos sociais, psicológicos e físicos das vítimas de *cyberbullying*?

A presente questão teve como objetivo identificar ações a promover no sentido de minimizar os diferentes danos que as vítimas de *cyberbullying* são sujeitas. Como Field (2018) demonstrou, o *cyberbullying* leva a uma predisposição para tendências suicidas, essencialmente em adolescentes, a quadros psiquiátricos como depressão e ansiedade, bem como ao abuso de substâncias psicoativas, aliando ainda os problemas físicos.

Neste caso as respostas foram diversas. O E1 começa por referir a necessidade de criação de canais de ajuda aos utilizadores, em que os ISP, com a colaboração de entidades competentes, teriam a capacidade de apoio e seguimento das vítimas de *cyberbullying*. O E3 menciona ainda a possibilidade de se efetuar uma avaliação do risco às vítimas, no sentido de as encaminhar para profissionais na matéria, e os E4 e E6, referem a sua necessidade de acompanhamento e apoio psicológico. Condutas bastante importantes, dado que, como se viu, existem especialistas que consideram o impacto psicológico e emocional provocado pelo *cyberbullying* potenciador de sentimentos de dor e sofrimento, de humilhação, raiva ou vulnerabilidade, com repercurções ao nível académico (Worthen, 2007 cit. por Figueiredo e Matos, 2017, pág. 126).

Neste âmbito, o E7 termina com a importância de reagir rapidamente e proteger a vítima, não esquecendo de ajudar o agressor a integrar-se na sociedade.

Também a referência à prevenção foi abordada, nomeadamente a sensibilização e a educação da sociedade sobre este fenómeno. Desde a identificação de potenciais vítimas ao acompanhamento da comunidade escolar, passando por uma "estratégia nacional" de formação nas escolas sobre a componente *cyber*, e até mesmo ao estudo das causas que levam os agressores a tais comportamentos, como referem, respetivamente, os E4, E5 e E7.

Considerando ainda o E6, se os conteúdos das agressões circularem em meio aberto, importa que qualquer pessoa denuncie e procure bloqueá-los de imediato, a fim de minimizar os danos nas vítimas, dado que quanto mais pessoas tiverem conhecimento, mais a vítima irá ser humilhada. A denúncia poderá dirigir-se aos OPC para investigação do crime, como diretamente aos prestadores de serviços de comunicações eletrónicas, que, perante conteúdos ilícitos, têm a obrigação de bloqueio imediato.

Perante os danos nas vítimas, o envolvimento imediato da Forças de Segurança é necessário, especialmente nos casos em que o cyberbullying representa uma séria ameaça à saúde mental e/ou física da vítima, sendo necessária uma cooperação rápida com ISP para identificar o infrator e impedir o crime (Vandebosch, Beirens, D'Haese, Wegge e Pabian, 2012).

Entrevistado	Conteúdo
E1	- (…) criação junto dos ISP, com o patrocínio das autoridades competentes de canais de ajuda aos utilizadores, com capacidade de apoio e seguimento será a solução mais adequada.
E2	- Esta é uma questão que escapa ao âmbito da ação do Ministério Público.
E3	- (…) avaliação do risco dirigido à vítima para a dirigir para grupos total ou parcialmente profissionalizados, como as Associações de Apoio à Vítima.
E4	- Pré-vitimização – sensibilização (online e presenciais), alerta, identificação de potenciais vítimas, através de proximidade e acompanhamento da comunidade escolar e também da sociedade em geral. Pós-sinalização/vitimização – Para além da necessária atividade de investigação criminal, todas as ações de acompanhamento próximo das vítimas, especialmente no apoio psicológico.
E5	- A existência de uma estratégia nacional de informação sobre a temática cyber nas escolas. - Os professores devem possuir as competências necessárias para lecionar estas matérias. - A existência nos currículos de conteúdos programáticos sobre o tema. - (…) transmitir aos mais novos a experiência do mundo real. - A informação e formação escolar.
E6	- (…) se circular no meio aberto, importa bloquear logo esse conteúdo para que os danos sejam os mínimos possíveis, para chegarem ao menor número possível de pessoas, dado que, a quanto mais pessoas chegar, mais a pessoa irá ser humilhada, os danos serão maiores. Portanto, atuação imediata no sentido de bloqueio imediato dos conteúdos, e isso é algo que qualquer pessoa pode fazer (…) . - Pode-se dirigir aos OPC para começarem a investigar porque se trata da prática de um crime, mas pode-se dirigir diretamente aos prestadores de serviços de comunicações eletrónicas para bloquearem esse conteúdo, porque se for um conteúdo manifestamente ilícito há essa obrigação de bloqueio imediato e portanto aí diminuímos o tipo de danos pela diminuição de pessoas que têm acesso à informação. Depois tem que haver um acompanhamento psicológico (…) para minimizar os danos psicológicos das vítimas.
E7	- (…) análise/estudo das causas que levam as pessoas a adotar tais comportamentos e de forma preventiva educar e formar os cidadãos para o direito (…). - Após a ocorrência, reagir de forma célere e visível para a vítima, o agressor e a sociedade percebam que a justiça é exercida atempadamente – num clik. - Proteger a vítima e garantir o apoio do agressor de forma a que este seja integrado na sociedade.

Quadro n.º 6 - Resumo das respostas à questão n.º 6 da Entrevista

Questão n.º 7

Considera que o conhecimento atempado pelas autoridades policiais de casos de *cyberbullying* permite minimizar os seus efeitos nas vítimas? Quais as razões?

Esta questão procurou essencialmente saber de que forma o conhecimento atempado pelas autoridades policiais de casos de *cyberbullying* permite minimizar os seus efeitos nas vítimas.

Os entrevistados foram perentórios em afirmar a importância desse conhecimento atempado. O *cyberbullying* destrói progressivamente as vítimas, daí que para os E1 e E2, o rápido conhecimento e a consequente primeira resposta, permitirá reduzir a agressão e as suas consequências na vítima. Assim como, permite levar ao exercício da justiça, cessando as agressões e demonstrando a sua eficácia, conforme manisfestado pelo E7. Atuações necessárias face à preocupação deixada por Amado et. al. (2009), dado que um *e-mail* ou uma mensagem podem ser

sucessivamente encaminhados para milhares de cibernautas, uma imagem, uma vez colocada em qualquer rede social, além de copiada e multiplicada, pode ficar eternamente no mundo virtual. Daí que o Facebook, para as situações que carecem de uma resposta imediata, nomeadamente as de perigo iminente, que prevejam risco de morte ou ferimentos graves, permite aos agentes da autoridade solicitar a intervenção da rede social para apoiar a vítima, através do Sistema de Pedidos *Online* para Autoridades.

O E4 reforça esta perspectiva, em que o conhecimento atempado proporcionará uma redução da vitimização, impedindo a evolução da violência e o impacto psicológico e físico na vitima. Por sua vez, o E6 fala do desconhecimento dos pais das vítimas em atuar nesta matéria, alertando para o facto de que poderão ser os OPC a intervir, orientando os pais em relação à forma de apoio, como psicológica e outras, bem como a solicitação do bloqueio imediato dos conteúdos ilicitos, a fim de minimizar os danos nas vítimas.

Conforme Antunes e Rodrigues (2018) referiram, após a partilha online de qualquer conteúdo que visa afetar alguém, a primeira preocupação consiste em estancar a sua difusão. Daí que a vítima, e em particular as autoridades policiais, deverão de imediato procurar que o conteúdo seja retirado dos servidores do prestador do serviço, especialmente se for numa rede social.

A produzirem o seu efeito, estes procedimentos pelas autoridades policiais tornam-se fundamentais no sentido de impedir maiores danos na vítima, dado que esses conteúdos poderão persistir no ciberespaço, serem replicados e potenciarem uma escalabilidade da agressão, não esquecendo que ainda poderão ser pesquizados e alvo de audiências desconhecidas. Tudo aquilo que é publicado fica na internet, assim como, a partir do momento em que se publique algo, perde-se o controlo desses conteúdos, existindo enorme potencial da sua visibilidade e consequentemente uma maior vitimização dos ofendidos (Seixas et al., 2016).

Atualmente as Forças de Segurança terão de evoluir, intervindo e garantindo também a segurança no ciberespaço. Devidamente especializadas e capazes de explorar as potencialidades dos sistemas informáticos, enquadradas na componente legal existente, terão de responder atempadamente às vítimas dos crimes informáticos. Conforme já referido, a Lei de política criminal mostra grande

preocupação em relação aos crimes praticados contra crianças e jovens, determinando como prioritário a proteção da vítima, a reparação dos danos e a garantia dos seus direitos.

Contudo, os E3 e E5, alertam para as possíveis dificuldades e borucracia que limitam a intervenção imediata das autoridades policiais, podendo surgir constragimentos na consumação dos objetivos de minimizar os efeitos das agressões nas vítimas, nomeadamente a possivel falta de cooperação das plataformas que guardam os dados na remoção dos conteúdos agressivos, alegando liberdade de expressão dos seus utilizadores.

Entrevistado	Conteúdo
E1	- (…) o conhecimento atempado pelas autoridades policiais e consequente primeira resposta é essencial para minorar quer a própria agressão quer os seus efeitos na vítima.
E2	- Claro que sim (…) O cyberbullying é insidioso, desgasta e corrói progressivamente as vítimas. Quanto mais rapidamente as autoridades souberem do caso e atuarem, menores serão as consequências da agressão.
E3	- Sim, se a esse conhecimento corresponder uma cooperação efetiva da plataforma que detém o depósito dos dados. (…) as plataformas alegam a existência de liberdade de expressão e isso tem constituído um problema para a efetivação da remoção.
E4	- Claro que sim. Impedirá o acentuar e agravar da vitimização, poderá prevenir uma escalada da violência e do impacto psicológico/físico na vítima e, em especial, permitirá uma recuperação (especialmente psicológica) da vítima mais eficaz.
E5	- As autoridades policiais quando têm conhecimento dos casos poderão esbarrar em algum procedimento burocrático de modo a por em causa, no imediato, a sua intervenção.
E6	- Sim, sem dúvida. - Em termos legais, se os pais não souberem como atuar (…) os OPC poderão fazê-lo e pedir o bloqueio imediato dos conteúdos, minimizando os danos nessa medida. (…) poderão orientar os pais, no caso de vítimas menores, quanto às principais formas de dar apoio a esses menores, como a parte psicológica e outras.
E7	- (…) o exercício célere da justiça permite minimizar os danos causados na vítima, terminar as ações do agressor, e demonstrar a eficácia da justiça.

Quadro n.º 7 - Resumo das respostas à questão n.º 7

Questão nº 8

Que mecanismos de resposta imediata, para a segurança e proteção das vítimas de *cyberbullying*, considera que seriam importantes desenvolver ao nível da intervenção no ciberespaço?

Por fim na última questão, procurou encontrar-se mecanismos de intervenção no ciberespaço, a fim de conseguir uma resposta imediata às vítimas de *cyberbullying*.

Na maioria dos entrevistados (E1, E2, E4, E5 e E7) foi possível verificar uma orientação para a possibilidade de se criarem processoas de cooperação, mesmo com

protocolos, envolvendo as diferentes entidades com responsabilidades na matéria, como autoridades judiciais, OPC, ISP, escolas, entre outros, a fim de se conseguir uma maior coordenação entre todas, no sentido de aumentar a eficácia no combate ao *cyberbullying*.

Contudo, pode verificar-se que alguns entrevistados foram mais objectivos nas suas respostas. O E1 realçou a importância dos ISP criarem mecanismos automáticos de controlo e remoção de conteúdos, através de métodos de alarme e descoberta, bem como a definição de procedimentos para a preservação e recolha de prova digital, não esquecendo nos casos detectados, a ajuda e apoio imediato à vítima. Racional partilhado nalguns estudos identificados, como de Yenurkar, Nandurkar, Thute, Shete (2018), que desenvolveram um algoritmo de correspondência de palavras, que procura identificar mais rapidamente as que se tornam abusivas/agressivas e ocultá-las da área de divulgação pública, no sentido de garantir um ambiente social mais saudável nas redes sociais.

Da mesma forma o E3 particulariza a componente tecnológica, neste caso mediante a aplicação de algoritmos para reconhecimento de linguagem e conteúdo potencial de imagens, assim como, pelo desenvolvimento de mecanismos de reporte imediato para classificação da informação abusiva, onde posteriormente um conjunto de pessoas confirmariam o abuso. Em particular por moderadores credenciados, onde as forças policiais deveriam fazer parte, a fim de melhorar a eficácia do mecanismo e a proteção da imagem da vítima, bem como pela garantia de um melhor contributo para as investigações.

Como reforço ao exposto pelo E3, o E4 realça também a existência de algoritmos que detetam em texto, imagem e vídeo, fenómenos de violência, e que enquadram medidas proativas levadas a cabo pelas redes sociais, permitindo uma "reposta e intervenção precoce junto da vítima e autor".

Noutra perspectiva, o E6 vem abordar a questão legal, nomeadamente pelo facto de se estar no momento a legislar sobre a protecção de direitos de autor, impondo-se regras às plataformas eletrónicas, nomeadamente pelo artigo 17.º da Directiva do Mercado Único Digital. Nesse sentido, deverá também ser criado algo para a proteção das vítimas de *cyberbullying*. Atualmente as plataformas electrónicas, como as redes sociais, afirmam que apenas fornecem uma plataforma "que os outros

utilizam para fazerem aquilo que bem quiserem, dizendo que nada têm a ver com os conteúdos". Daí que o E6 "acreditaria num artigo 17.º mais facilmente para a proteção dos menores e das vítimas de *cyberbullying*, o que implicaria criar uma obrigação destas plataformas vigiarem ativamente as suas redes e os seus serviços de maneira a impedirem que o *cyberbullying* tivesse lugar". Ainda a nivel legal, o E6 defende uma legislação que torne mais rápidas e claras as medidas de acesso aos endereços de IP e a outros dados de tráfego que permitam identificar o agressor.

Por fim, aborda-se ainda outra prespectiva deixada pelos E5 e E6, nomeadamente em relação à possível intervenção de imediato pelas autoridades. Onde para o E5 é importante ao nível dessas autoridades a "existência de equipas, ou elementos especialistas, formados para o efeito, que possam interagir de imediato". Já o E6 direciona essa intervenção imediata para os OPC´s, realçando também a importância da existência de equipas especializadas para intervir em cenários de *cyberbullying*, que reúnam a sensibilização necessária e a capacidade de reencaminhar as vítimas e os pais para os meios mais adequados, e que saibam atuar perante terceiros, como seja os prestadores de serviço de comunicações eletrónicas, no sentido de bloquearem logo os conteúdos, bem como, que saibam de imediato pedir-lhes a conservação dos dados necessários para identificação do agressor, porque se os agressores forem logo identificados menos atuam no dia seguinte.

Da análise efetuada aos atuais mecanismos de resposta ao *cyberbullying*, verifica-se que não existe diretamente uma capacidade de primeira resposta que garanta eficazmente a segurança e proteção das vítimas, no sentido de minimizar os efeitos e danos das agressões virtuais e que combata os fatores cibernéticos pontenciadores deste tipo de agressões.

Entrevistado	Conteúdo
E1	- (…) importante a criação de protocolos efetivos de cooperação entre as entidades com responsabilidade no combate ao cyberbulling e os ISP, a criação por estes de mecanismos automáticos de controlo e remoção de conteúdos, com alarmística e heurística, bem como a criação de procedimentos para a preservação e recolha de prova digital, sem descorar a ajuda e apoio imediato (pós incidente) à vítima.
E2	- (…) coordenação de todos os interlocutores: as polícias com as escolas, em primeira linha e depois as polícias com o Ministério Público. A intervenção do Ministério Público é essencial, (…) muitas das diligências de obtenção de prova (digital) dependem de autorização do Ministério Público.
E3	- Desde a aplicação de algoritmos para reconhecimento de linguagem, a algoritmos de reconhecimento de conteúdo potencial de imagens, a mecanismos de reporte imediato para

	classificação da informação abusiva com possibilidade de aprendizagem automática pelas plataformas, como forma de chamada de intervenção por um conjunto de pessoas que confirmem o abuso. Por exemplo, adoção de um mecanismo semelhante ao existente dos jogos em linha, onde existem moderadores credenciados que fiscalizam comportamentos. (…) as forças policiais poderiam vir a fazer parte desses moderadores (…) seria mais eficaz. Aceleraria a proteção da imagem da vítima e redundava em melhores investigações.
E4	- Já vão existindo algoritmos que detetam (em texto, imagem e vídeos) fenómenos de violência. Este tipo de medidas proativas (acompanhadas de ação humana para deteção de publicações que não são detetadas) são levadas a cabo pelas plataformas de social media e permitem uma reposta e intervenção precoce junto da vítima e autor. - É essencial, pelas autoridades públicas e também pelo setor privado, trazer o assunto do cyberbullying para fora do ambiente e comunidade escolar e assumir uma postura de combate a estes fenómenos que envolva toda a sociedade.
E5	- Uma maior cooperação entre autoridades policiais e judiciais. - Ao nível das autoridades, existência de equipas, ou elementos especialistas, formados para o efeito, que possam interagir de imediato. - Os operadores e os prestadores do serviço de comunicações eletrónicas deverão ter elementos, formados para o efeito, como pontos de contato das autoridades judiciais e policiais permitindo tornar mais eficiente este tipo de combate.
E6	- Assim como está criado e quase a entrar em vigor o artigo 17º da Diretiva do Mercado Único Digital, que se dirige à proteção de direitos intelectuais, ou seja, impedir a violação de direitos de autor e que impõe regras às plataformas eletrónicas, pelo menos essas, também faz sentido criar algo para a proteção as vitimas de cyberbullying. - Falámos que, temos de um lado os meios de comunicação tradicionais (…) Do outro lado oposto temos os meros ISP que fornecem o acesso à internet e que nada tem a ver com os conteúdos propriamente ditos, e depois temos aquele espaço que está no meio, das plataformas (…) a fornecer uma plataforma que os outros utilizam para fazerem aquilo que bem quiserem, dizendo que nada têm a ver com os conteúdos. A posição destes é que nada têm a ver com os conteúdos, sendo uma posição que querem salvaguardar. - A primeira grande legislação sobre esta matéria tem dado aso a grandes polémicas é esta do mercado único digital que visa a proteção dos direitos de autor, Julgo que teria muito mais sentido, já que vamos mexer nestes que estão no meio para os responsabilizar pelos conteúdos, muito mais sentido faz na questão da proteção dos mais desfavorecidos, mais desprotegidos, como sejam as vitimas de cyberbullying (…). - Portanto, acreditaria num artigo 17 mais facilmente para a proteção dos menores e das vítimas de cyberbullying, o que implicaria criar uma obrigação destas plataformas vigiarem ativamente as suas redes e os seus serviços de maneira a impedirem que o cyberbullying tivesse lugar. - Portanto criaria uma lei mais clara, para tornar mais rápida e mais clara as medidas de acesso aos endereços de IP e a outros dados de tráfego que permitiriam identificar o agressor. - Os OPC deviam ser especializados, deviam ter equipas especializadas para isso. (…) para terem sensibilização e poderem reencaminhar as vitimas e os pais para os meios mais adequados, e que soubessem atuar perante terceiros, como seja os prestadores de serviço de comunicações eletrónicas, no sentido de bloquearem logo os conteúdos, que soubessem logo pedir-lhes a conservação dos dados necessários para identificação do agressor, porque se os agressores fossem logo mais facilmente identificados menos atuariam no dia seguinte.
E7	- Identificar instituições com capacidades de responder às necessidades da vítima e identificar, eventualmente através de protocolos, processos de trabalho entre as instituições de apoio e os OPC.

Quadro n.º 8 - Resumo das respostas à questão n.º 8

4. CONCLUSÕES E REFLEXÕES

4.1. Conclusões

O presente capítulo procura apresentar, por um lado, as principais conclusões, tendo em conta os objetivos propostos no início do presente estudo e tecer algumas recomendações na ótica de propostas de futuras investigações científicas nesta área como também a apresentação de algumas linhas estratégicas de desenvolvimento de uma capacidade de intervenção ciberpolicial.

Ao longo da investigação procurou-se cumprir o OG - identificar e caracterizar a primeira resposta às vítimas de *cyberbullying*, contributo importante para o conhecimento e a necessária resposta a este flagelo.

Como resposta a este objetivo, verificou-se o seguinte: a importância de garantir uma maior aplicação e cumprimento das regras jurídicas para a preservação da vítima e garantia dos seus direitos; o desenvolvimento de uma conduta proactiva dos ISP no combate ao *cyberbullying*; a garantia de uma sociedade mais sensibilizada sobre este fenómeno, associada a uma maior cooperação entre os diferentes intervenientes; e por fim, de realçar a necessidade de existir uma capacidade ciberpolicial para cessar de imediato as agressões virtuais, garantindo o apoio às vítimas e a recolha dos dados inerentes às agressões.

Para alcançar esse OG, aplicou-se o modelo de análise já referenciado, que teve por base as PD formuladas a partir da PP, que se procede à sua resposta.

PD1 - De que forma poderão ser cessadas as agressões virtuais de *cyberbullying*?

Começa-se pela necessidade dos ISP disporem de mecanismos automáticos, como algoritmos de deteção de texto e imagem, essencialmente as redes sociais, para controlo de conteúdos abusivos que enquadrem casos de *cyberbullying*, garantindo uma capacidade de bloqueio e identificação dos seus autores. Esse controlo automático deverá ainda sinalizar conteúdos suspeitos, lançando preventivamente alertas para o ofendido e agressor, contribuindo para a cessação destas agressões. Deverão também os utilizadores das redes sociais procurar o uso das ferramentas aí

existentes para denúncia e eventual bloqueio de agressões virtuais, que levarão à análise desses conteúdos no sentido de se verificar o incumprimento dos termos de uso e a consequente remoção dos mesmos, bem como uma eventual eliminação dos seus autores. Daí que surge a necessidade de um maior conhecimento sobre o fenómeno, sobre as TIC e sobre a vivência no ciberespaço, para que as vítimas possam proteger-se ou efetuarem rapidamente denúncia às autoridades policiais.

Poderá igualmente contribuir para a cessação das agressões, o desenvolvimento de canais de comunicação e de ajuda imediatos, com a respetiva intervenção de especialistas, levando a que as denúncias permitam a identificação imediata das agressõess virtuais e à consequente intervenção dos ISP responsáveis, bloqueando e/ou removendo esses conteúdos. Se as agressões virtuais circularem em áreas públicas, os ISP têm a obrigação de intervir, por iniciativa própria ou por solicitação das autoridades públicas.

PD2 - De que forma poderão ser identificados os autores de agressões virtuais de *cyberbullying*?

Os mecanismos existentes são os aplicáveis à maioria dos crimes informáticos ou cibercrimes, seguindo-se os trâmites legais definidos no ordenamento jurídico, perante as solicitações oficiais das autoridades competentes no âmbito das investigações em curso.

Os IPS deverão garantir os mecanismos tecnológicos necessários para efetuar o controlo e identificação da origem dos conteúdos abusivos. Em caso de necessidade e de perigo para as vítimas, os IPS poderão ainda remeter essa identificação através de uma ação oficiosa para as autoridades competentes em caso de deteção.

Da mesma forma, e quando possível para o caso em apreço, poderão os OPC de imediato pedir a guarda e conservação dos dados ao ISP, enquanto que a junção ao processo, em determinados casos, terá de ser por pedido do Ministério Público ou Juiz de Instrução.

É bastante importante que os ISP tenham consciência da necessidade de preservarem os dados relevantes e os divulgarem rapidamente às autoridades policiais, a fim de se conseguir de forma célere e eficaz intervir para proteger a vítima e recuperar o agressor.

Para melhorar estas comunicações deveriam ser criados canais ou pontos de contacto, a fim de se procurar uma comunicação imediata e a aquisição da informação de forma mais célere. Para o efeito, poder-se-ia oficializar essa colaboração e os pontos de contacto, garantindo um comprometimento com a causa e a existência de especialistas em ambas as partes para o tratamento deste fenómeno.

PD3- Quais os mecanismos para obter prova das agressões virtuais de *cyberbullying*?

De forma geral, a obtenção da prova digital das agressões virtuais passará pela aplicação e o cumprimento das regras jurídicas de preservação e obtenção de dados de comunicações.

Contudo, considera-se bastante importante que as autoridades policiais solicitem de imediato aos ISP a preservação e o fornecimento dos conteúdos e endereços IP do agressor/cliente que lá os colocou.

Este tipo de prova deve ser recolhida na sua origem, evitando adulteração da mesma, daí a importância dos ISP garantirem a sua preservação e disponibilização. A título de exemplo, a rede social Facebook prevê nas suas políticas a disponibilização de informação para responder a emergências, mediante pedido das autoridades competentes. Caso essa informação não seja garantida num espaço de tempo curto, pelo menos fica o registo para que seja preservada e bloqueada, a fim de salvaguardar os direitos da vítima e minimizar os danos causados. Para facilitar, poderá mesmo solicitar-se a celebração de protocolos para no futuro agilizar procedimentos e reduzir tempo e burocracia. O que importa de imediato são as medidas cautelares de preservação de prova e proteção da vítima.

Existem estudos que reforçam a importância das FS intervirem no *cyberbulling*, em particular na cessação do crime, passando pela identificação do agressor e na ajuda da vítima, e em particular, removendo os conteúdos nocivos e agressivos. Mas importa que haja melhores procedimentos internacionais, como princípios de retenção para todos os ISP, procedimentos adequados de notificação, remoção e obtenção da necessária prova digital. Para essa intervenção poderá contribuir o desenvolvimento de uma componente policial cibernética, direcionada para estes fenómenos interpessoais como *cyberbullying*.

PD4 - Quais as ações a serem tomadas para apoiar as vítimas de agressões virtuais de *cyberbullying*?

Em primeiro lugar, a necessidade de existirem normas legais que imponham aos ISP a obrigação de vigiarem ativamente as suas redes e os seus serviços para prevenirem casos de *cyberbullying*, e que garantam mais rapidamente o acesso aos endereços de IP e a outros dados de tráfego que permitam identificar os agressores.

Para além da importância das vítimas se protegeram, importa também que qualquer pessoa denuncie e procure de imediato bloquear os conteúdos agressivos. Daí que, como noutros problemas, é necessária a sensibilização e educação da sociedade sobre este fenómeno.

A possibilidade de se criarem processos de cooperação, envolvendo as diferentes entidades com responsabilidades na matéria, como autoridades judiciais, OPC, ISP, escolas, entre outros, permite criar uma cooperação e coordenação que poderá aumentar a eficácia no combate ao *cyberbullying*, em particular na deteção e proteção das vítimas.

Os ISP deverão adotar medidas proativas, em especial as redes sociais, que permitam uma intervenção precoce junto da vítima e do agressor. Deverão garantir a implementação de mecanismos tecnológicos de deteção e reporte das agressões virtuais, no sentido de proteger a vítima e contribuir para a persecução da justiça, bem como, criarem canais de ajuda aos utilizadores, para que com a colaboração de entidades competentes terem a capacidade de apoio às vítimas.

Por fim, dos contributos reunidos, verifica-se a importância do envolvimento imediato dos OPC, surgindo daí a necessidade de se desenvolver uma capacidade ao nível das FS para intervir em cenários de *cyberbullying*, reunindo elementos especializados que consigam interagir e intervir de imediato junto das vítimas e agressores. Esta capacidade deverá ter o conhecimento necessário para acompanhar e encaminhar as vítimas e os familiares para as instâncias adequadas. Da mesma forma, que garanta ainda a imediata coordenação com os ISP para cessar o crime, conservar e bloquear os conteúdos ilícitos. Para contribuir para esta resposta, as FS deverão desenvolver canais de denúncia e reporte imediatos, que permitam ter acesso em tempo real à informação da ocorrência, de modo a conseguir a redução da vitimização dos ofendidos, impedindo a evolução da violência e o impacto

psicológico e físico nas vítimas. Não obstante, esta capacidade de resposta permitirá efetuar uma avaliação do risco às vítimas, no sentido de, dentro das suas necessidades imediatas, as apoiar ou encaminhar para os profissionais adequados.

PP - Qual a resposta imediata que as vítimas de *cyberbullying* necessitam?

Pelo desenvolvimento da investigação, parte-se da premissa que o *cyberbullying* necessita de uma reação rápida para garantir a maior proteção da vítima e minimizar os danos da agressão sofrida, dado que uma agressão virtual poderá ser tanto maior quanto mais tempo permanecer no ciberespaço. Daí que a primeira preocupação seja impedir a sua visualização e difusão por outros utilizadores, procurando de imediato que seja retirada dos servidores do ISP, em particular se for uma rede social.

Desta forma, é importante que se garanta a aplicação e o cumprimento das regras jurídicas para a preservação da vítima e garantia dos seus direitos, passando pela repressão dos agressores.

É necessária uma maior resposta dos ISP no combate ao cyberbullying, mediante uma conduta proativa e uma melhor colaboração com as autoridades competentes para o bloqueio das agressões virtuais e o fornecimento dos dados necessários.

Atualmente, deverá existir uma sociedade mais sensibilizada e instruída sobre este fenómeno, para que qualquer pessoa denuncie e procure de imediato bloquear os conteúdos agressivos que levam ao cyberbullying.

A criação processos de cooperação, envolvendo as diferentes entidades com responsabilidades na matéria poderá aumentar a eficácia no combate ao cyberbullying, em particular na deteção e proteção das vítimas.

Foi ainda possível identificar a necessidade de existir de uma capacidade "Ciberpolicial" para, em colaboração com os ISP, cessarem de imediato o crime, reunirem os dados necessários para confirmarem a agressão e identificarem os autores, e consequentemente, apoiarem as vítimas nas suas necessidades imediatas.

4.2. Reflexões

Uma das principais reflexões da presente investigação prende-se com a falta de algum controlo do ambiente digital, seja pelos ISP ou pelas autoridades policiais.

O contexto das comunicações digitais facilita o *cyberbullying*, que, associado ao constante desenvolvimento das TIC, tem potenciado as agressões virtuais. Importa assim atuar no espaço vazio, procurando junto de vítimas e agressores, uma intervenção personalizada e adaptada a cada situação, no sentido de gerar um clima de confiança. Como se viu, aquando das ocorrências de *cyberbullying*, há que de imediato promover junto das vítimas a sua proteção e segurança, mas garantindo a sua privacidade, e aos agressores, a sua recuperação, sem que ambos se sintam condicionados no acesso às TIC, mais ainda estando na presença de nativos digitais. Condições estas que, face às medidas a tomar, exigem uma resposta das FS.

Nesse sentido, considerando a proximidade e a confiança que Guarda Nacional Republicana garante junto dos cidadãos, aliado ao facto de ter manifestado[35] a intenção de incrementar a capacidade de atuação no ciberespaço para garantir uma resposta integrada ao fenómeno da cibercriminalidade no mundo real e virtual, poderá vir a desenvolver esta capacidade policial, ou mesmo uma "CiberGuarda", para intervir nestes casos de *cyberbullying*.

Para o desenvolvimento deste tipo capacidade ciberpolicial, considera-se que deverá ser criada uma estrutura com meios humanos e materiais específicos, e que se mantenha enquadrada no normativo legal em vigor, no sentido de poder garantir a resposta adequada às vítimas.

Independentemente da ordem jurídica atribuir à Polícia Judiciária a exclusividade de investigação dos crimes informáticos, a particularidade dos crimes que enquadram o *cyberbullying* levam uma necessidade premente de intervenção imediata para salvaguarda a vítima, nomeadamente impedindo ou minimizando de imediato os danos na mesma, fruto da escalabilidade que a agressão poderá ter em virtude das características do ciberespaço e das funcionalidades das redes sociais. Ora, para o conceito de "*first responding*" que se pretende, poderão ser as FS a

[35] *In* Sistemas de Informação, Revista Pela Lei e Pela Grei da GNR. Edição outubro-dezembro de 2015.

garantir esta capacidade de resposta no âmbito das suas atribuições cautelares e de polícia, considerando o seu contacto imediato com as vítimas e as necessárias medidas cautelares, prévias à investigação.

Para o cabal funcionamento desta capacidade de resposta pelas FS, salienta-se a necessidade de se constituírem equipas com o treino e conhecimento adequado, nomeadamente, policial, de psicologia criminal (para crianças e jovens de diferentes faixas etárias) e informático de utilizador avançado (dominar a área da prova digital e informática forense). A estrutura de comando e direção desta capacidade deverá ter conhecimentos avançados de direito e informática, e ainda, estreitas ligações a diferentes entidades com relevância na matéria (CSIRT, policiais, segurança social, entre outros). Importa ainda que, face à vivência virtual e às práticas criminais aí existentes, esta capacidade ciberpolicial crie a tal estreita e necessária ligação aos ISP, em especial às redes sociais, para cooperação e partilha de informação, essencialmente para a cessação do crime, identificação do agressor e ajuda à vítima, particularmente para a remoção dos conteúdos nocivos e agressivos.

Face à conjuntura atual, esta capacidade ciberpolicial permitiria combater os comportamentos desviantes, entre crianças e jovens, mais frequentes no ciberespaço, através de uma intervenção imediata, constituída por elementos treinados, com disponibilidade 24h por dia e apta a detetar, reprimir e apoiar os intervenientes.

Não obstante, deverá ainda ser criado um "canal de comunicação" para ajudar na operacionalização da resposta às vítimas. Esse canal deverá ser específico para estes casos, no sentido de aumentar a confiança na denúncia, permitindo desta forma o acesso às equipas especializadas, para que de imediato ocorram a estes casos e garantam uma resposta eficaz, com a devida privacidade da vítima.

Esta resposta às vítimas de *cyberbullying* poderá também vir ser dada e adaptada a outras vítimas de ofensas a partir das TIC, dado que os crimes que estão na base do *cyberbullying* também ocorrem por toda a sociedade.

Considera-se que se deverá continuar a garantir a proximidade e resposta ao cidadão, procurando incrementar e acompanhar a segurança e proteção da população na era digital, e assim, que as funções policiais se mantenham operacionais no ciberespaço, acompanhando a evolução dos tempos, que tem migrado pessoas, identidades, práticas socias e criminais para o mundo virtual.

Prevendo-se que, futuramente, toda a população, para além de estar conectada virtualmente, irá também desenvolver muitas das suas atividades no mundo virtual. Torna-se assim importante que todos os responsáveis por garantir "segurança", desenvolvam os estudos e investigações necessárias para garantir o seu estado digital, e que desta forma acompanhem a evolução da sociedade.

BIBLIOGRAFIA

Livros

Antunes, M. & Rodrigues, B. (2018). *Introdução à Cibersegurança: A Internet, os Aspectos Legais e a Análise Digital Forense* (1ª ed.). Lisboa: FCA – Editora de Informática.

Asher, J. (2017). *Por treze razões* (11ª ed.). Lisboa: Editorial Presença.

Quivy, R. & Campenhoudt, L. V. (2008). *Manual de investigação em Ciências Sociais*. Lisboa: Gradiva.

Sarmento, M. (2013). *Metodologia Científica para a Elaboração, Escrita e Apresentação de Teses*. Lisboa: Universidade Lusíada Editora.

Schmidt, E. & Cohen, J. (2013). *A Nova Era Digital: Reformulando o Futuro das Pessoas, das Nações e da Economia* (1ª ed.). Alfragide: Dom Quixote.

Seixas, S., Fernandes, L., & Morais, T. (2016). *Cyberbullying: Um guia para pais e educadores*. (1ª ed.). Lisboa: Plátano Editora.

Venâncio, P. (2011). *Lei do Cibercrime* (1ª ed.). Lisboa: Coimbra Editora, S.A.

Vilelas, J. (2009). *Investigação: o processo de construção do conhecimento*. Lisboa: Edições Sílabo.

Artigos

Amado, J., Matos, A., Pessoa, T., & Jäger, T. (2009). Cyberbullying: Um desafio à investigação e à formação. *Interações*, 13, pp. 301-326. Obtido de: https://revistas.rcaap.pt/interaccoes/article/view/409.

Deviet, M. (2018, Mar-Abr). Fuzzy Based Genetic Operators for Cyber Bullying Detection Using Social Network Data. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 3 (3), pp. 437-444. Obtido de: http://ijsrcseit.com/CSEIT1833243.

Field T. (2018, agosto). Cyberbullying: A narrative review. *Journal of Addiction Therapy and Research*, 2, pp. 10-27. Obtido de: https://dx.doi.org/10.29328/journal.jatr.1001007.

Figueiredo, F. & Matos, A. (2017). Agressão apoiada pelas tecnologias: O cyberbullying e o autocyberbullying. *Interações*, 45, pp. 119-150. Obtido de: https://revistas.rcaap.pt/interaccoes/article/view/7137.

Gabinete Cibercrime da Procuradoria-Geral da República (2013). TU E A INTERNET (AB)USO, CRIME E DENÚNCIA. Obtido de: http://www.ministeriopublico.pt/ebook/tu-e-internet.

Guedes, A. & Santos, L., (2015, julho/dezembro). Breves reflexões sobre Poder e Ciberespaço. *Revista de Direito e Segurança*, 6, pp. 189–209. Obtido de: https://comum.rcaap.pt/bitstream/10400.26/14329/1/PodereCiberesa%C3%A7o.pdf

Haoti Zhong, H.L., Squicciarini, A., Rajtmajer, S., Griffin, C., Miller, D. & Caragea, C. (2016) Content-Driven Detection of Cyberbullying on the Instagram Social Network. *Proceedings of the Twenty-Fifth International Joint Conference on Artificial Intelligence*, pp. 3952-3958. Obtido de: https://www.ijcai.org/Proceedings/16/Papers/556.pdf.

Matos, A., Pessoa, T., Amado, J. & Jäger, T. (2011). Agir contra o Cyberbullying – Manual de Formação. *Congresso Nacional "Literacia, Media e Cidadania"*. Braga: Centro de Estudos de Comunicação e Sociedade da Universidade do Minho. ISBN 978-989-97244-1-9. Obtido de: http://www.lasics.uminho.pt/OJS/index.php/lmc/article/view/463/434.

Monteiro, S. (2016, abril). Stratεgia 21: fec2c8175a4ba67cb187958a639fa6ed*. *Revista da Armada*, 506, pp. 4-5.

Monteiro, S. (2016, maio). Stratεgia 22: Cibersegurança e ciberdefesa – Portugal e NATO. *Revista da Armada*, 507, pp.4-5.

Natário, R. (2013, outubro). O Combate ao Cibercrime: Anarquia e Ordem no Ciberespaço. *Revista Militar*, 2541. Obtido de: https://www.revistamilitar.pt/artigo/854.

Neto, A. A. L. (2005). Bullying - comportamento agressivo entre estudantes. *Jornal de Pediatria*, 81(5), pp. 164-172. Obtido de: http://www.scielo.br/pdf/%0D/jped/v81n5s0/v81n5Sa06.pdf.

Nunes, P. V. (2014). Ciberespaço, ciberviolência e o uso organizado da força. *Janus Anuário*, 3.33, 146-147. Obtido de:

http://janusonline.pt/images/anuario2014/3.33_PauloVNunes_Ciberespaco.pdf.

Pessoa, T. & Amado, J. (2014). Cyberbulling - Questões e desafios atuais. *edmetic, Revista de Educación Mediática y TIC*, 3 (2), E-ISSN: 2254-0059, pp. 29-51. Obtido de: https://dialnet.unirioja.es/descarga/articulo/5192023.pdf.

Smith, P.K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippet, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry*, 49(4), pp. 376-385. Obtido em: https://onlinelibrary.wiley.com/doi/epdf/10.1111/j.1469-7610.2007.01846.x.

Vandebosch, H., Beirens, L., D'Haese, W., Wegge, D., & Pabian, S. (2012). Police actions with regard to cyberbullying: The Belgian case. *Psicothema*, 24 (4), pp. 646-652. Oviedo: Universidade de Oviedo. Obtido de: http://www.redalyc.org/articulo.oa?id=72723959022.

Yenurkar, T., Nandurkar, A., Thute, N. & Shete, R. (2018, março). Abused Word Detection on Social Media. *International Journal on Future Revolution in Computer Science & Communication Engineering*, 4 (3), pp. 85-87. Obtido de: http://www.ijfrcsce.org.

Trabalhos

Cruz, A. C. C. (2011). *O Cyberbullying no contexto português* (Dissertação no âmbito do Mestrado em Ciências da Comunicação, variante Estudos dos Media e de Jornalismo). Lisboa: Faculdade de Ciências Sociais e Humanas da Universidade Nova de Lisboa. Obtido de: https://run.unl.pt/bitstream/10362/5958/1/disserta%c3%a7ao%20mestrado%20cyberbullying.pdf.

Ferreira, E. P. T. C. P. (2018). *As crianças e o Bullying: A relação do estatuto socioprofissional dos pais e a diferença entre géneros* (Dissertação no âmbito do Mestrado em Psicologia Clínica e de Aconselhamento). Lisboa: Universidade Autónoma de Lisboa. Obtido de: http://repositorio.ual.pt/bitstream/11144/3778/1/Disserta%c3%a7%c3%a3o.pdf.

Gabinete Cibercrime (2017). Nota Prática nº 11/2017 de 2 de novembro. In portal do *Ministério Público*. Obtido de: http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_11_jurisprudencia_penal_substantiva.pdf.

Gómez-Adorno, H., Bel-Enguix, G., Sierra, G., Sanchez, O. & Quezada, D. (2018). *A Machine Learning Approach for Detecting Aggressive tweets in Spanish.* Third Workshop on Evaluation of Human Language Technologies for Iberian Languages. Mexico City: Universidad Nacional Autónoma de México, Engineering Institute. Obtido de: https://scholar.google.pt/scholar?q=A+Machine+Learning+Approach+for+Detecting+Aggressive+tweets+in+Spanish.&hl=ptPT&as_sdt=0&as_vis=1&oi=scholart.

Montalvão, N. M. M. (2015). *Cyberbullying: Caracterização do fenómeno em Portugal*. (Dissertação no âmbito do Mestrado em Crime, Diferença e Desigualdade). Braga: Instituto de Ciências Sociais da Universidade do Minho. Obtido de: http://repositorium.sdum.uminho.pt/bitstream/1822/40722/1/Nuno%20Manuel%20Martins%20Montalv%c3%a3o.pdf.

Pinheiro, L. O. (2009). *Cyberbullying em Portugal: uma perspectiva sociológica* (Dissertação no âmbito do Mestrado em Sociologia: desenvolvimento e politicas sociais). Braga: Instituto de Ciências Sociais da Universidade do Minho. Obtido de: http://repositorium.sdum.uminho.pt/bitstream/1822/9870/1/tese.pdf.

Risch, J., Krestel, R. (2018). *Aggression Identification Using Deep Learning and Data Augmentation*. First Workshop on Trolling, Aggression and Cyberbullying at the 27th International Conference of Computational Linguistics. Germany: University of Potsdam. Obtido de: https://www.researchgate.net/publication/326548433_Aggression_Identification_Using_Deep_Learning_and_Data_Augmentation.

Santos, J. L. A. (2011). *Contributos para uma melhor governação da cibersegurança em Portugal* (Dissertação no âmbito do Mestrado em Direito e Segurança).

Lisboa: Faculdade de Direito da Universidade Nova de Lisboa. Obtido de: https://run.unl.pt/bitstream/10362/7341/1/Santos_2011.PDF.

Santos, J. L. A. (2017). *Cibersegurança. Aula 1 da Unidade Curricular – Cibersegurança, no âmbito do Mestrado em Direito e Segurança 2016/2017*. Lisboa: Faculdade de Direito da Universidade Nova de Lisboa.

Simas, D. V. (2014). *O Cibercrime* (Dissertação de Mestrado em Ciências Jurídico-Forenses). Lisboa: Universidade Lusófona de Humanidades e Tecnologias. http://recil.grupolusofona.pt/xmlui/handle/10437/5815.

Viegas, C. S. A. C. (2017). *As vítimas de violência doméstica e os fenómenos do Stalking, Cyberstalking e do Bullying* (Dissertação de Mestrado em Direito). Lisboa: Universidade Autónoma de Lisboa. Obtido de: http://repositorio.ual.pt/bitstream/11144/3855/1/Correc%c3%a7%c3%b5es%20Disserta%c3%a7%c3%a3o%20-%20Catarina%20Viegas.pdf.

Legislação

Assembleia da República (1995). Código Penal: Decreto-Lei n.º 48/95, de 15 de março, com as alterações introduzidas pela Lei n.º 44/2018, de 09 de agosto. Obtido de: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=109&tabela=lei.

Assembleia da República (2004). Lei do Comércio Electrónico no Mercado Interno e Tratamento de dados pessoais: Decreto-Lei n.º 7/2004, de 07 de janeiro, com as alterações introduzidas pela Lei n.º 46/2012, de 29 de agosto. Obtido de: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1399&tabela=leis&.

Assembleia da República (2009). Lei do Cibercrime: Lei n.º 109/2009, de 15 de setembro. Obtido de: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis.

Assembleia da República (2008). Lei de Organização da Investigação Criminal: Lei n.º 49/2008, de 27 de agosto. Obtido de: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1021&tabela=leis&.

Assembleia da República (2017). Lei de Política Criminal – Biénio de 2015-2017: Lei n.º 96/2017, de 23 de agosto. Obtido de: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2761&tabela=leis&.

Conselho da Europa (2014). Guia dos Direitos Humanos para os Utilizadores da Internet: Recomendação CM/Rec (2014)6 do Comité de Ministros aos Estados-Membros. 1197.ª reunião dos Delegados dos Ministros. Obtido de: https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-cm-rec-2014-6-of-the-committee-of-ministers-to-member-states-on-a-guide-to-human-rights-for-internet-users-adopted-by-the-committee-of-?inheritRedirect=false. Consultado em 17nov18.

União Europeia (2016). Regulamento 2016/679 do Parlamento Europeu e do Conselho de 27 de abril: Proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial das Comunidades Europeias, n.º L 119.

Webgrafia

https://about.twitter.com/pt/safety.html. Consultado em 27nov18.

http://cibercrime.ministeriopublico.pt. Consultado em 31dec18.

https://dicionario.priberam.org/emoji.

https://help.instagram.com/426700567389543/?helpref=hc_fnav&bc[0]=Ajuda%20do%20Instagram&bc[1]=Centro%20de%20Privacidade%20e%20Seguran%C3%A7a. Consultado em 26nov18.

http://linhaalerta.internetsegura.pt/index.php. Consultado em 17nov18.

https://olhardigital.com.br/noticia/facebook-nao-e-mais-a-rede-social-mais-usada-para-ciberbullying/69837. Publicação de Juliana Américo (19/07/2017, 16H50). Consultado em 03Nov18.

https://pt-pt.facebook.com/safety/groups/law/guidelines/. Consultado em 26nov18.

https://support.google.com/youtube/answer/2802268?hl=pt&ref_topic=2803176. Consultado em 27nov18.

https://www.anacom.pt/render.jsp?contentId=430538. Consultado em 31dec18.

https://www.cncs.gov.pt/sobre-nos/missao-e-competencias/. Consultado em 30dec18.

https://www.facebook.com/safety/groups/law/guidelines/. Consultado em 03nov18.

https://www.internetsegura.pt/. Consultado em 17nov18.

http://www.pgdlisboa.pt. Consultado várias vezes entre 2018 e 2019.

https://www.policiajudiciaria.pt/unc3t/. Consultado em 31dec18.

https://www.snap.com/pt-PT/safety/safety-center/. Consultado em 27nov18.

https://www.whatsapp.com/security/. Consultado em 27nov18.

APÊNDICES

Apêndice A - Modelo de análise e Questões do Inquérito por Entrevista

OBJETIVOS	PERGUNTAS	QUESTÕES DO INQUÉRITO POR ENTREVISTA
OG: Identificar e caracterizar a primeira resposta às vítimas de *cyberbullying*.	**PP:** Qual a resposta imediata que as vítimas de *cyberbullying* necessitam?	
OE1: Descrever como se poderão cessar as agressões virtuais de *cyberbullying*.	**PD1:** De que forma poderão ser cessadas as agressões virtuais de *cyberbullying*?	1. Face à particularidade do cyberbullying, de que forma poderiam ser cessadas as agressões virtuais e minimizados os seus efeitos nas vitimas? 2. Como poderão os Internet Service Providers (ISP) (redes sociais, links, plataformas de e-mail) procurar o bloqueio, rastreabilidade e remoção dos conteúdos ilícitos no ciberespaço?
OE2: Descrever como se poderão identificar os autores de agressões virtuais de *cyberbullying*.	**PD2:** De que forma poderão ser identificados os autores de agressões virtuais de *cyberbullying?*	3. Quais os mecanismos técnicos e legais que poderão possibilitar a identificação dos autores de *cyberbullying*? 4. De que forma poderão os ISP colaborar com as as autoridades policiais na identificação do perfil ou conta dos autores do *cyberbullying*?
OE3: Identificar os mecanismos para recolher e preservar a prova digital de agressões virtuais de *cyberbullying*.	**PD3:** Quais os mecanismos para obter prova das agressões virtuais de *cyberbullying*?	5. De que forma poderá ser obtida a prova digital das agressões virtuais efetuadas contra as vítimas de *cyberbullying*?
OE4: Identificar as ações que poderão ser tomadas para apoiar as vítimas de agressões virtuais de *cyberbullying*.	**PD4:** Quais as ações a serem tomadas para apoiar as vítimas de agressões virtuais de *cyberbullying*?	6. Quais as ações e e em que momento, dentro e fora do ciberespaço, deverão ser desenvolvidas para minimizar os danos sociais, psicológicos e físicos das vítimas de *cyberbullying*? 7. Considera que o conhecimento atempado pelas autoridades policiais de casos de *cyberbullying* permite minimizar os seus efeitos nas vitimas? Quais as razões? 8. Que mecanismos de resposta imediata, para a segurança e proteção das vitimas de *cyberbullying*, considera que seriam importantes desenvolver ao nivel da intervenção no ciberespaço?

Apêndice B - Carta de Apresentação e Guião do Inquérito por Entrevista

CARTA DE APRESENTAÇÃO

No âmbito da dissertação do curso de Mestrado em Direito e Segurança da Faculdade de Direito da Universidade Nova de Lisboa, subordinada ao tema, "*Cyberbullying*: A primeira resposta às vítimas", vimos por este meio solicitar a V. Ex.ª a melhor colaboração para a realização de uma entrevista, no sentido de recolher informações e esclarecimentos decorrentes da investigação.

A presente entrevista permitirá reunir conhecimentos que serão um contributo preponderante para se atingir os objetivos propostos neste trabalho. Para a sua realização foram privilegiados especialistas na área do direito, do apoio a vítimas, do cibercrime e das Tecnologias de Informação e Comunicação.

Tendo em consideração os imperativos relativos à proteção de dados, todos os requisitos de identificação dos entrevistados serão tratados de forma confidencial.

Grato pela sua colaboração e disponibilidade.

Atenciosamente,

Gonçalo Nuno Correia Zambujo Serrão

Lisboa, março de 2019

GUIÃO DE ENTREVISTA
"Cyberbullying: A primeira resposta às vítimas"

1. IDENTIFICAÇÃO DO(A) ENTREVISTADO(A)

Nome:

Organização:

Departamento:

Função:

Local:

Data/Hora (início/fim):

2. ENQUADRAMENTO

O *cyberbullying* tem levado a sociedade a investir na prevenção do fenómeno, no entanto, ao nível da intervenção após a ocorrência, muito ainda se poderá realizar para dar uma resposta imediata às vítimas e minimizar os efeitos das agressões virtuais.

Perante a conjuntura atual, importa olhar para o ciberespaço e encontrar a possibilidade de uma intervenção no problema o mais precoce possível, antes que ele se desenvolva e crie mais danos na vítima. Impõem-se mais ações para preservar a vítima, nomeadamente a sua imagem social, integridade emocional, psíquica e até física.

3. ENTREVISTA

1. Face à particularidade do *cyberbullying*, de que forma poderiam ser cessadas as agressões virtuais e minimizados os seus efeitos nas vítimas?
2. Como poderão os Internet Service Providers (ISP) (redes sociais, *links*, plataformas de *e-mail*) procurar o bloqueio, rastreabilidade e remoção dos conteúdos ilícitos no ciberespaço?
3. Quais os mecanismos técnicos e legais que poderão possibilitar a identificação dos autores de *cyberbullying*?
4. De que forma poderão os ISP colaborar com as as autoridades policiais na identificação do perfil ou conta dos autores do *cyberbullying*?
5. De que forma poderá ser obtida a prova digital das agressões virtuais efetuadas contra as vítimas de *cyberbullying*?
6. Quais as ações e em que momento, dentro e fora do ciberespaço, deverão ser desenvolvidas para minimizar os danos sociais, psicológicos e físicos das vítimas de *cyberbullying*?
7. Considera que o conhecimento atempado pelas autoridades policiais de casos de *cyberbullying* permite minimizar os seus efeitos nas vítimas? Quais as razões?

8. Que mecanismos de resposta imediata, para a segurança e proteção das vítimas de *cyberbullying*, considera que seriam importantes desenvolver ao nível da intervenção no ciberespaço?

Obrigado.

Apêndice C - Entidades Entrevistadas

Entrevistado/a (E)	Entrevistados	Função	Data
E1	Inspetor Baltazar Rodrigues	Inspetor e Especialista em cibercrime e Informática Forense da PJ	15-03-2019
E2	Procurador Pedro Verdelho	Coordenador do Gabinete Cibercrime da Procuradoria Geral da República	25-03-2019
E3	Inspetor-Chefe Rogério Bravo	Coordenador da área do cibercrime na UNC3T da PJ	07-04-2019
E4	Major Rogério Raposo	Coordenador do Departamento de Operações do Centro Nacional de Cibersegurança - CERT.PT	12-04-2019
E5	Dr. António Rolhas	Consultor Superior Principal na ANACOM	09-04-2019
E6	Professora Doutora Sofia Casimiro	Professora de Direito na Academia Militar e Coordenadora de projetos de Ciberdefesa	29-04-2019
E7	Tenente-Coronel Paulo Poiares	Chefe da Divisão de Emprego Operacional da GNR e formador de *Cyberbullying*	01-05-2019